

User's Manual

Gigabit Multi-Homing VPN Security Gateway

▶ MH-2300



Copyright

Copyright © 2014 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer

manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

WEEE Regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual of PLANET Gigabit Multi-Homing VPN Security Gateway
Model: MH-2300
Rev: 1.0 (December, 2014)
Part No. EM-MH-2300_v1.0

Table of Contents

Chapter 1. Installation	7
1.1 Hardware Installation	7
1.2 Basic System Configuration	7
Chapter 2. System	14
2.1 Administration.....	14
2.1.1 Admin	15
2.1.2 Permitted IPs.....	17
2.1.3 Logout	17
2.1.4 Software Update.....	18
2.2 Configuration	18
2.2.1 Settings	21
2.2.2 Date / Time.....	25
2.2.3 Multiple Subnets	26
2.2.4 Routing Table	31
2.2.5 DHCP	34
2.2.6 Dynamic DNS	36
2.2.7 Host Table.....	37
2.2.8 Language.....	38
Chapter 3. Interface	39
3.1 Interface	39
3.1.1 Examples of Interface.....	44
Chapter 4. Policy Object	73
4.1 Address.....	73
4.1.1 Examples of Policy Creating.....	75
4.2 Service	80
4.2.1 Example of Custom Service.....	81
4.2.2 Example of Service Group	85
4.3 Schedule	86
4.3.1 Examples of Schedule.....	87
4.4 QoS.....	89
4.4.1 Example of Bandwidth Limitation	90
4.5 Authentication.....	93
4.5.1 Local / Group Authentication.....	99
4.5.2 RADIUS Authentication	102
4.5.3 POP3 Authentication	123
4.5.4 LDAP Authentication	125

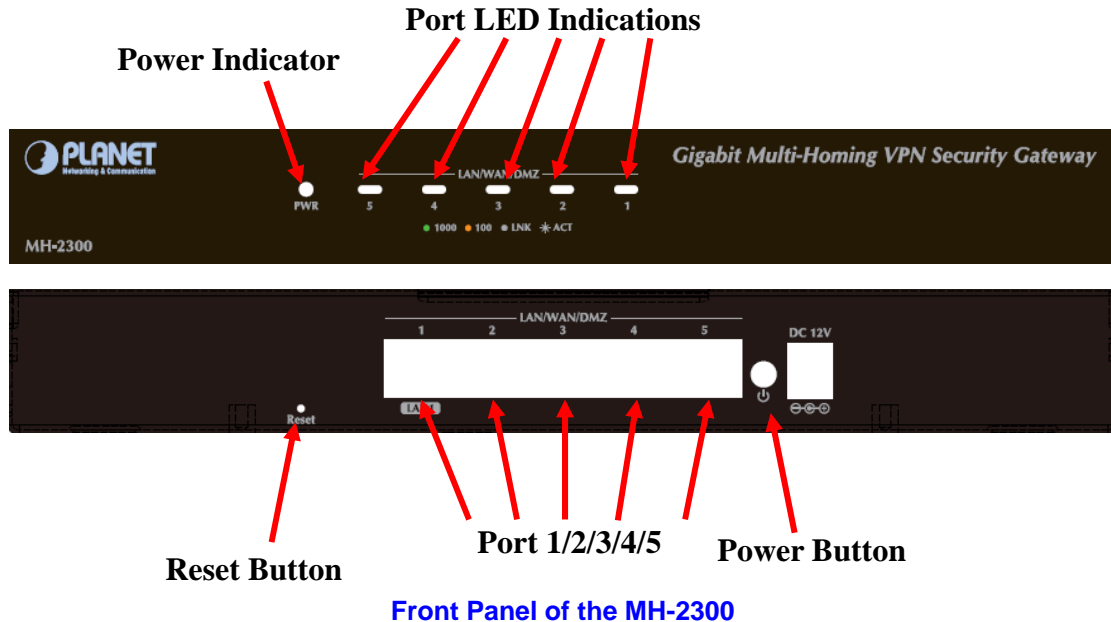
4.6 Application Blocking	147
4.6.1 Examples of Blocking	149
4.7 Virtual Server	152
4.7.1 Examples of Virtual Server	153
4.8 VPN	169
4.8.1 Examples of VPN	178
Chapter 5. Web Filter	305
5.1 Configuration	305
5.1.1 Examples of Web Filter	309
5.2 Reports	319
5.2.1 Statistics	323
5.2.2 Logs	325
Chapter 6. Policy	326
6.1 Policy	326
6.1.1 Example	330
Chapter 7. Abnormal IP Flow	348
7.1 Abnormal IP Flow	348
7.1.1 Example	348
Chapter 8. Monitoring	351
8.1 Logs	351
8.1.1 Traffic	352
8.1.2 Events	355
8.1.3 Connections	356
8.1.4 Application Blocking	358
8.1.5 Concurrent Sessions	360
8.1.6 Quota	362
8.1.7 Logging Settings	364
8.2 Traffic Grapher	366
8.2.1 WAN Traffic	367
8.2.2 Policy-based Traffic	369
8.3 Diagnostic Tools	371
8.3.1 Ping	371
8.3.2 Traceroute	374
8.4 Wake-on-LAN	375
8.4.1 Example	375
8.5 Status	376
8.5.1 Interface	379

8.5.2	System Info	381
8.5.3	Authentication.....	381
8.5.4	ARP Table	382
8.5.5	Sessions Info	383
8.5.6	DHCP Clients.....	383


Chapter 1. Installation

1.1 Hardware Installation

Front Panel:



- **Power Indicator:** Lights up in green when the power is on.
- **Port 1 / 2 / 3 / 4 / 5** can be defined as:
 - ◆ LAN Port: For connecting to a switch.
 - ◆ WAN Port: For connecting to a perimeter router.
 - ◆ DMZ Port: For providing the public with services, such as email or Web, using a physically-separated network segment, while at the same time preventing any potential security threats.
- **Power Button:** For turning MH-2300 on or off.
- **Reset Button:** For resetting MH-2300 to factory default settings.

 Note	<p>1. Port LED Indications:</p> <ul style="list-style-type: none"> ■ Flashing indicates the packets are processed through the device. Amber indicates a link speed at 10/100 Mbps. Green indicates a link speed at 1000 Mbps. <p>2. The reset button is an SMT component; please don't press it too hard. Otherwise, damage to reset function may happen.</p>
----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.2 Basic System Configuration

Step 1. Connect the IT administrator's network adaptor and MH-2300's LAN port to the same hub / switch, and then launch a browser (IE or Firefox) to link the management interface at <http://192.168.1.1>.

Step 2. The browser prompts you for the login credentials. (Both are “admin” by default.)

Typing in the User Name and Password

Step 3. The user interface consists of the following two panels:

- **Menu Panel:** Presents all the available system configurations in a tree directory structure. (See Overview of Functions for further details)
- **Configuration Panel:** Displays the data or configurable settings of the corresponding item selected on the **Menu Panel**.

System > Configuration > Installation Wizard

Step5: Settings Confirmation

Confirm the settings made from previous steps. Click **Finish** to complete the installation when confirmed. If not, click **Back** to modify settings.


Port	Name	Forwarding Mode	IP Address / Netmask
1	LAN1	NAT	192.168.0.1 / 255.255.255.0
2	Port2	---	0.0.0.0 / 0.0.0.0
3	Port3	---	0.0.0.0 / 0.0.0.0
4	Port4	---	0.0.0.0 / 0.0.0.0
5	WAN1	Static IP	192.168.1.162 / 255.255.255.0

Menu Panel

Configuration Panel

< Back Finish >

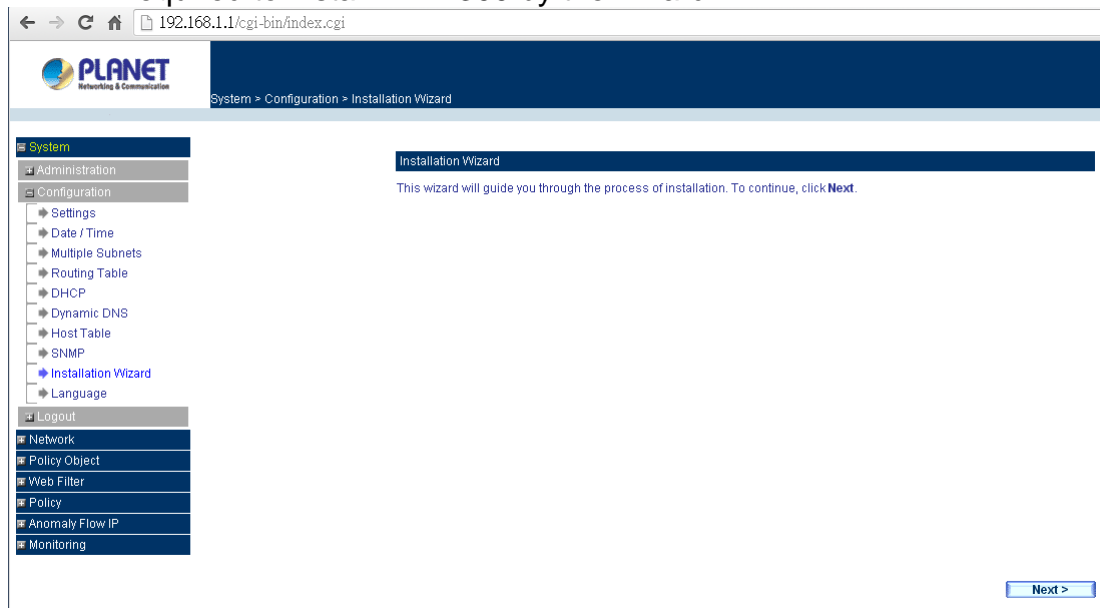
The MH-2300's Management Interface


Note

For your reference, you may configure your management address based on the available subnet ranges below.

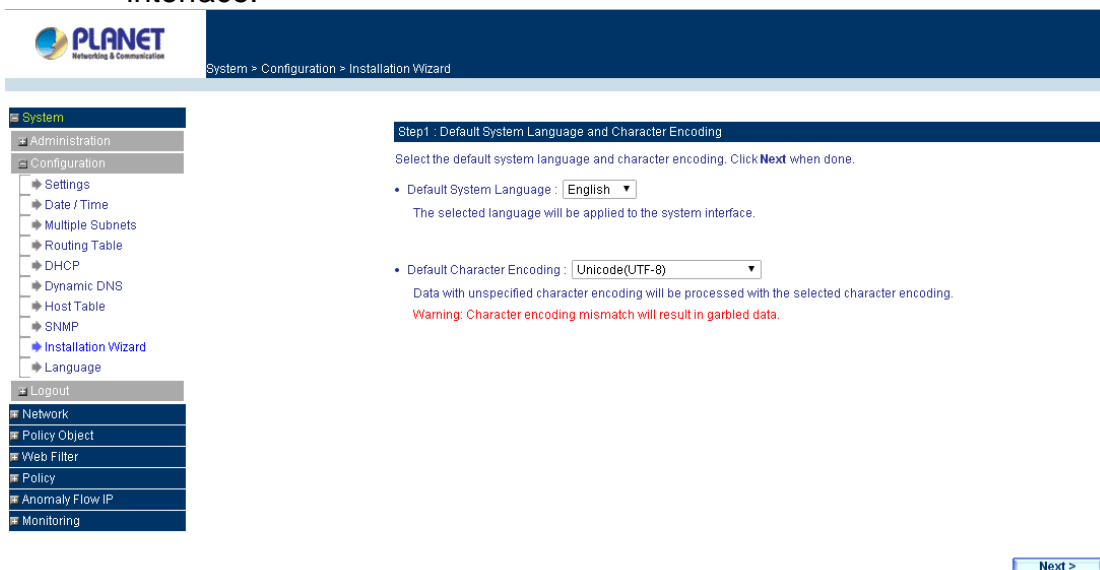
10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

Step 4. At the first login, you will be guided through the basic settings that are required to install MH-2300 by the wizard.



The Install Wizard

Step 5. Select the language and character encoding for your management interface.



Selecting the Language and Default Character Encoding



The default encoding will be applied to the data of unspecified encoding.

Port Configuration

Step 1. Configure the LAN settings: (according to your network infrastructure).

- **Physical Connection:** Select "Port1 (LAN1)".
- **Interface Type:** Select "LAN".
- **Connection Type:** Select "NAT Routing".
- Specify the **IPv4 Address** and **Netmask**.

Step2 : Interface Settings

Configure the interface settings for physical connections respectively. Click **Next** when done.

Physical Connection : Port1 ▼

Interface Settings

Interface Designation : LAN1

Interface Type : ☐ Disabled ☒ LAN ☐ WAN ☐ DMZ

Connection Type : NAT Routing ▼ Help

IPv4 Settings

IPv4 Address : 192.168.1.1

Netmask : 255.255.255.0

MAC Address : A8:F7:E0:11:22:33

IPv6 Settings

Connecting using : Auto-configuration ▼

IPv6 Address :

Prefix Length : 0

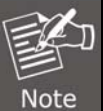
☐ Enable Any IP Routing Help

Access by / via : Help ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

< Back

Next >

Configuring the LAN Interface Settings



The access to the management interface is subject to the LAN interface. Therefore, enter the management address to a Web browser correspondingly if any changes have been made to the LAN interface.

Step 2. Configure the WAN Interface (please refer to your ISP for the details).

- Select "Port 5 (WAN 1)" for **Physical Connection**.
- Select "WAN" for **Interface Type**.
- Select your **Connection Type**.

■ Complete the remaining fields according to your network.

Step2 : Interface Settings

Configure the interface settings for physical connections respectively. Click **Next** when done.

Physical Connection : **Port5** ▼

Interface Settings	
Interface Designation : WAN1	
Interface Type : <input type="radio"/> Disabled <input type="radio"/> LAN <input checked="" type="radio"/> WAN <input type="radio"/> DMZ	
Connection Type : <input checked="" type="radio"/> Static IP Address (Leased Line User) <input type="radio"/> Dynamic IP Address (Cable Modem User) <input type="radio"/> PPPoE (ADSL Dial-Up User)	
IPv4 Settings	
IPv4 Address :	211.21.21.21
Netmask :	255.255.255.0
IPv4 Default Gateway :	211.21.21.254
MAC Address :	A8:F7:E0:11:22:33
IPv6 Settings	
Connecting using :	Auto-configuration ▼
IPv6 Address :	
Prefix Length :	
IPv6 Default Gateway :	
Max. Downstream Bandwidth :	512 Mbps (1 - 1000)
Max. Upstream Bandwidth :	512 Mbps (1 - 1000)
Keepalive Properties :	
Help	Type : DNS ▼
	DNS IP Address : 8.8.8.8
	Domain Name : 8.8.4.4 (Max. 55 characters)
	Minimum Interval : 5 second(s) (0 - 99, 0: no detection)
NAT Redirection : Auto-configuration ▼	
Help	
Access by / via :	
Help	<input checked="" type="checkbox"/> Ping/Tracert <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Telnet <input checked="" type="checkbox"/> SSH

< Back

Next >

Configuring the WAN Interface Settings

Step 3. Tick the box of **“Synchronize to an NTP server”** to ensure the accuracy of system clock.

System > Configuration > Installation Wizard

System time : Fri, Nov 14 11:53:27 2014

Step3 : Synchronization Settings

To ensure the reliability of recorded data, configure the time zone and synchronization settings. Click **Next** when done.

• Time Zone Setting :

The hours offset from GMT: [Assist Me](#)

• Synchronization Settings :

☒ Synchronize to an NTP server

☐ Observe daylight-saving time from / To /

Server IP or Hostname [Assist Me](#)

Update Interval: minutes (0 – 99999, 0: updated when system reboot)

[< Back](#)

[Next >](#)

Configuring the System Clock Settings

Step 4. Tick the box of **“Outgoing”** to create a policy for outgoing traffic.

System > Configuration > Installation Wizard

Step4 : Default Policy Settings

Select your desired policy types to create required policies. Click **Next** when done.

☒ Outgoing

☐ Incoming

☐ WAN to DMZ

☐ LAN to DMZ

☐ DMZ to WAN

☐ DMZ to LAN


☐ LAN to LAN

☐ DMZ to DMZ

[< Back](#)

[Next >](#)

Creating an Outgoing Network Policy


Note

1. After the completion of wizard, an outgoing network policy is created correspondingly under Policy > Outgoing.

- Source Address is defaulted to "Inside_Any".
- Destination Address is defaulted to "Outside_Any".
- Service is defaulted to "Any".

Source	Destination	Service	Action	Options	Configuration
Inside Any	Outside Any	Any	✓		Modify Remove Pause

[New Entry](#)

The Policy Allowing LAN Users to Access External Network Resources

2. To allow Internet access to LAN users, assign their PCs with static IP addresses within the same subnet as MH-2300 as well as designate MH-2300 as the default gateway. Otherwise, enable DHCP service to automatically distribute IP addresses to them. LAN traffic can be regulated by means of network policies if desired.

Step 5. This step confirms what interface addresses have been assigned to MH-2300.

Network > Interface

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.1.1 / 255.255.255.0	---	Modify	---
2	Port2	---	0.0.0.0 / 0.0.0.0	---	Modify	---
3	Port3	---	0.0.0.0 / 0.0.0.0	---	Modify	---
4	Port4	---	0.0.0.0 / 0.0.0.0	---	Modify	---
5	WAN1	Static IP	211.21.21.21 / 255.255.255.0	---	Modify	1

Confirmation on Interface Settings

Step 6. Installation is completed after clicking **Finish** from the previous step.

Chapter 2. System

2.1 Administration

This chapter will cover the configuration of *Admin*, *Permitted IPs*, *Software Update* and *Logout*. The default administrator serves as a system administrator, who is allowed to modify configuration, monitor operational status, and access system reportings, whereas sub-administrators are subject to the access privileges permitted. A sub-administrator with full privileges can be seen as a system administrator.

Terms in Admin

Admin Name

- The authentication name for system login.
- The login credentials for the system administrator are both defaulted to “admin”, which are not available for medication or deletion.

Access Privilege

- The system administrator “admin” is allowed to modify configuration, manage administrative accounts, and access system reporting.
- The capability of a sub-administrator is subject to the access privileges permitted. The access privilege of a sub-administrator can be specifically assigned on an individual basis. It is suggested to assign a sub-administrator with either “Read” or “Read/View” privilege (“View” allows for accessing system reporting).

Password / New Password / Confirm Password

- Add or modify the password of an administrative account.

2.1.1 Admin

2.1.1.1 Adding a Sub-Administrator

Step 1. Under **System > Administration > Admin**, set as shown below:

- Click the **New Sub-Admin** button to create a new sub-administrator.
- Specify the login credentials, respectively.
- Repeat the **Password** in the **Confirm Password** field.
- Tick **Read** under the **Access Privilege** section.
- Click **OK**.

Add Sub-Admin
Help

Sub-Admin Name : (Max. 20 characters)


Password : (Max. 20 characters)

Confirm Password : (Max. 20 characters)

Access Privilege

	<input checked="" type="checkbox"/> Read	<input type="checkbox"/> Read/Write	<input type="checkbox"/> Log Content
System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policy Object	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Web Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Anomaly Flow IP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitoring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Adding a Sub-Admin



Note

Hierarchical management can be achieved by assigning the access privilege such as read/ write access to a system setting or the browsing of log contents to the sub-administrator specifically on an individual basis.

2.1.1.2 Modifying the Password

Step 1. Under **System > Administration > Admin**, set as shown below:

- Click **Modify** corresponding to the administrative account to be modified.
- Enter the current and the new passwords, respectively.
- Repeat the **Password** in the **Confirm Password** field.
- Select the **Access Privilege**.
- Click **OK**.

Modify Sub-Admin Password and Privilege Help

Sub-Admin Name : Sub-Admin

Password : (Max. 20 characters)

New Password : (Max. 20 characters)

Confirm Password : (Max. 20 characters)

Access Privilege

	<input checked="" type="checkbox"/> Read	<input type="checkbox"/> Read/Write	<input type="checkbox"/> Log Content
± System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Policy Object	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Web Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Anomaly Flow IP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
± Monitoring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK
Cancel

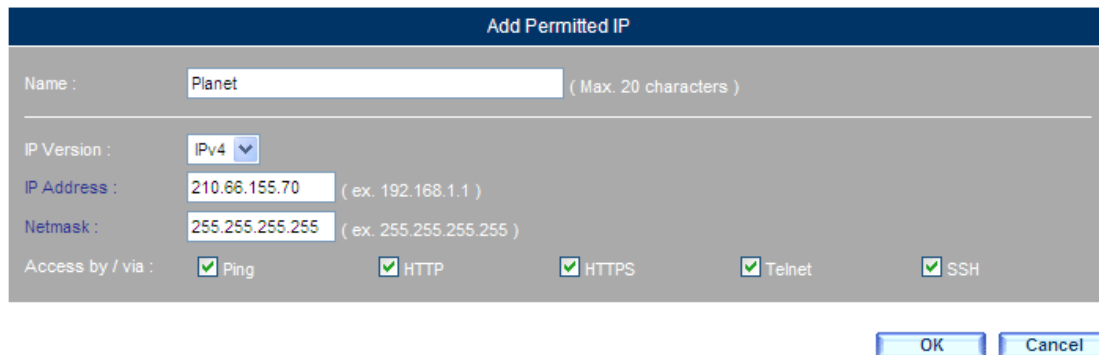
Modifying the Password and Access Privileges

2.1.2 Permitted IPs


2.1.2.1 Adding a Permitted IP

Step 1. Under **System > Administration > Permitted IPs**, click **New Entry** and then set as shown below:

- Specify a name for the permitted IP.
- Select **“IPv4”** for **IP Version**.
- Enter the IP address.
- Enter the netmask. (“255.255.255.255” indicates a single IP address)
- **Access by / via** : Select **Ping/ Tracert, HTTP** and **HTTPS**.
- Click **OK**.



Adding a Permitted IPs



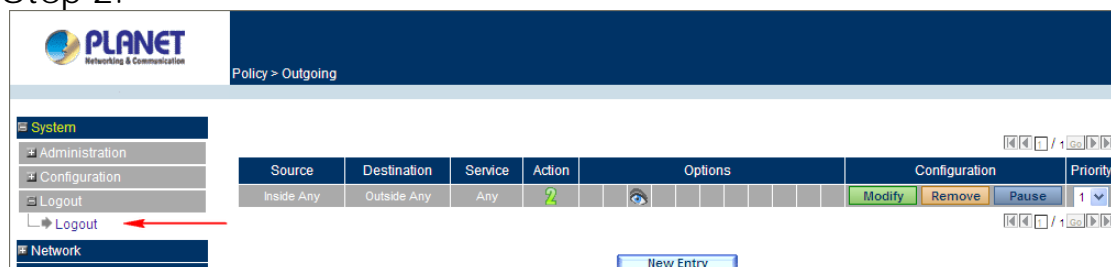
1. For Permitted IPs to be effective, it requires to uncheck the boxes of **Ping, HTTP, HTTPS, Telnet** and **SSH**.
2. At least a permitted IP must be configured prior to the cancellation of **HTTP** and **HTTPS** boxes; otherwise, the management interface will be inaccessible.

2.1.3 Logout

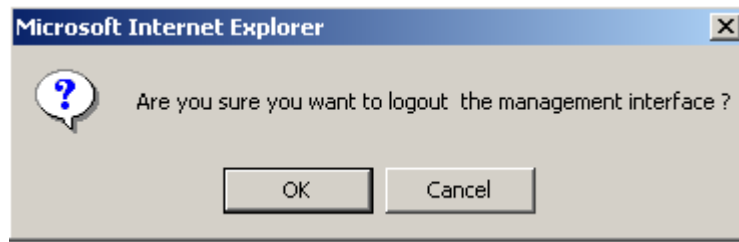
2.1.3.1 Logging out the System

Step 1. Click **Logout** under **System > Logout** to prevent system from unauthorized access or being tampered with.

Step 2.



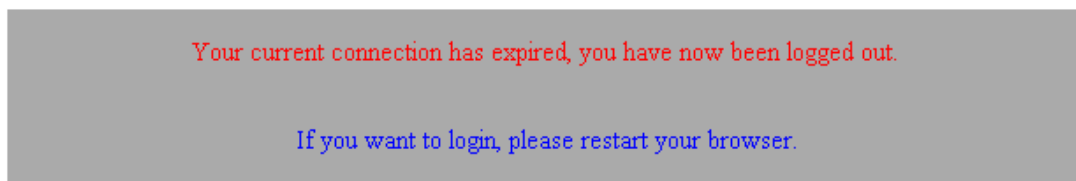
Logging out the System



Confirming to Log Out

Step 3. A message is shown after confirming the logout.

MH-2300 Information

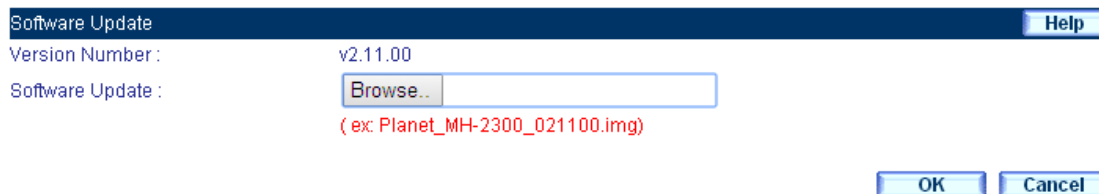


The Logout Message

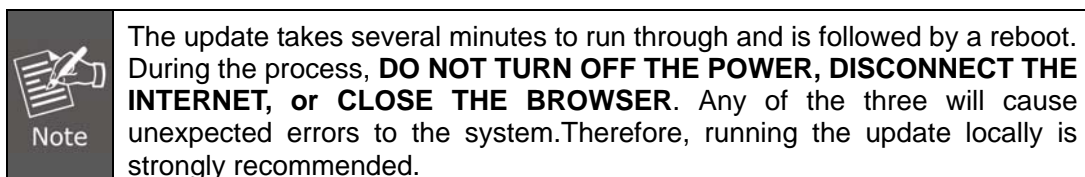
2.1.4 Software Update

Step 1. To run a software update, go to **System > Administration > Software Update** and follow the steps below:

- Click **Browse** to locate the software.
- Click **OK** to proceed the update.



Updating the Software



2.2 Configuration

This chapter will cover the configuration of *Settings, Date / Time, Multiple Subnets, Routing Table, DHCP, Dynamic DNS, Host Table, and Language.*

Terms in Settings

System Settings

- Allowed for importing / exporting the system configuration file and resetting system to factory default settings.

Configuration File Backup and Restore Utility

- Allowed for performing backups of system configuration and restore from a specific date (depending on the availability of backup). This feature efficaciously helps avert the corruption or damage of system configuration file.
- The backup can be achieved automatically at 00 : 00 hours on a daily basis or manually in a timely manner.
- All configuration file backups can be downloaded onto a local computer for archival purpose.

Name Settings

- Type a device name and your company name, respectively.

Email Notification Settings

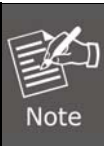
- When enabled, system notification and reporting can be emailed to the designated recipient(s).

Syslog Message Settings

- Allowed for sending syslogs generated by system operation.

Management Interface Settings

- Enables the device to be remotely accessed through a browser over connection protocols, including HTTP(S), Telnet, and SSH. The port number for each protocol is customizable according to your needs.
- Specify a period of time in the **Idle Timeout** field to automatically log out an idle administrative account ("idle" refers to no action is performed).
- Specify an amount of time to limit the consecutive failed login attempts and a period of time to block the IP address of a user who has exceeded the limit.



Once the HTTP(S) port for external access has been modified, then it will require appending the new port number to the management address to access the system, such as `http://61.62.108.172:8080` or `https://61.62.108.172:1025`.

SIP/ H.323 NAT Traversal Settings

- Allowed for enabling SIP or H.323 NAT traversal.

System Reporting Storage Time

- Assign a storage time for the system utilization info under **Monitoring > Status > System Info**.

Page Display Configurations

- Determine the items displayed per page for policy objects and operation logs (e.g., Web filtering, etc.).
- Determine the default charset for generating system reporting. It is intended for data with unspecified encoding.

Device Reboot

- The MH-2300 unit can be manually rebooted or scheduled to reboot at a specified time.

Terms in Date / Time

Synchronization Settings

- The system clock can be synchronized to an NTP server or a local computer.

GMT

- It is short for Greenwich Mean Time, the international standard time.

Daylight Saving Time

- Daylight saving time (DST; also summer time) is the portion of a year in which a region's local time is advanced by an hour from its standard official time.

Terms in Multiple Subnets

Name

- Specify a name for the subnet.

Interface

- Designate an interface (i.e., LAN or DMZ) that the subnet connects to.

IP Version

- Specify the IP addressing method used.

Alias IP Address (IPv6 Address) / Netmask(Prefix Length)

- Specify the corresponding IP address range.

Terms in Routing Table

Static Routing

- Provides a static route based on the administrator's configuration settings or a default route.
- Provides IPv4/ IPv6 addressing capability.

Terms in DHCP

Static IP Assignment

- Allowed for distributing IP addresses to internal PCs based on their MAC address.

Terms in Dynamic DNS

Domain Name

- The domain name registered at a dynamic DNS provider.

Real IP Address

- The real IP address that the domain name corresponds to.

Terms in Host Table

Hostname

- A user-definable name for a host that is accessible to internal users.

IP Version

- Specify the IP addressing method used.

IP Address

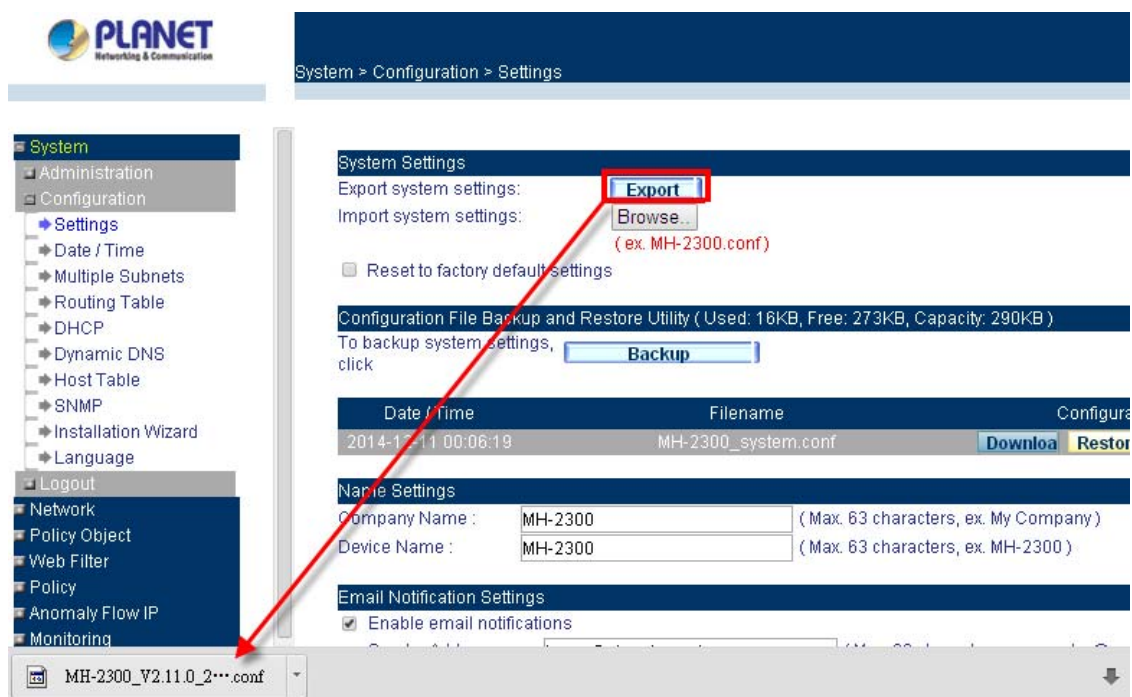
- A LAN or DMZ IP address that the host name corresponds to.

2.2.1 Settings

2.2.1.1 Exporting System Settings

Step 1. Under **System > Configuration > Settings**, set as shown below:

- Click **Export** under the **System Settings** section.
- The configuration will download automatically.



The screenshot displays the Planet MH-2300 web management interface. The breadcrumb navigation at the top indicates the path: **System > Configuration > Settings**. On the left, a sidebar menu shows the 'System' section expanded, with 'Settings' selected. The main content area is titled 'System Settings' and includes an 'Export' button, which is highlighted with a red rectangle and a red arrow. Below this, there is a section for 'Configuration File Backup and Restore Utility' with a 'Backup' button. Further down, 'Name Settings' and 'Email Notification Settings' are visible. At the bottom of the interface, a download bar shows a file named 'MH-2300_V2.11.0_2...conf' with a download icon.

Exporting System Settings as a File

2.2.1.2 Importing System Settings

Step 1. Under **System > Configuration > Settings**, set as shown below:

- Click **Browse...** under the **System Settings** section.
- In the **Choose file** dialogue box, select the configuration file and then click **Open**.
- Click **OK**.
- Click **OK** to confirm importing the file.

System Settings Help

Export system settings: Export

Import system settings: Browse... MH-2300_V2.1...0141211.conf
(ex. MH-2300.conf)

☐ Reset to factory default settings

Configuration File Backup and Restore Utility (Used: 32KB, Free: 257KB, Capacity: 290KB) Help

To backup system settings, click Backup

Date / Time	Filename	Configuration		
2014-12-11 00:06:19	MH-2300_system.conf	Download	Restore	Remove
2014-12-11 06:34:26	MH-2300_V2.11.0_20141211.conf	Download	Restore	Remove

Name Settings Help

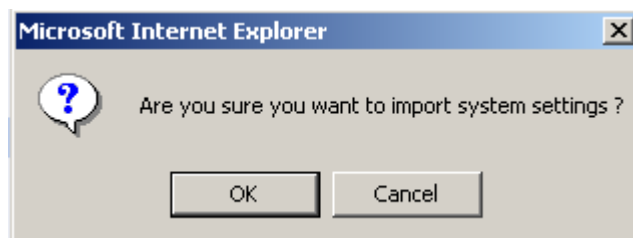
Company Name : (Max. 63 characters, ex. My Company)

Device Name : (Max. 63 characters, ex. MH-2300)

Email Notification Settings Help

☒ Enable email notifications

Selecting the System Settings File to Import



Confirming to Import the System Settings

2.2.1.3 Resetting the System to Factory Settings

Step 1. Under System > Configuration > Settings, set as shown below:

- Tick **Reset to factory default settings** under the **System Settings** section.
- Click **OK** at the lower right corner to proceed.
- Click **OK** in the confirmation box to execute the procedure.



System Settings Help

Export system settings: Export

Import system settings: Browse... MH-2300_V2.1...0141211.conf
(ex. MH-2300.conf)

☒ **Reset to factory default settings**

Configuration File Backup and Restore Utility (Used: 32KB, Free: 257KB, Capacity: 290KB) Help

To backup system settings, click Backup

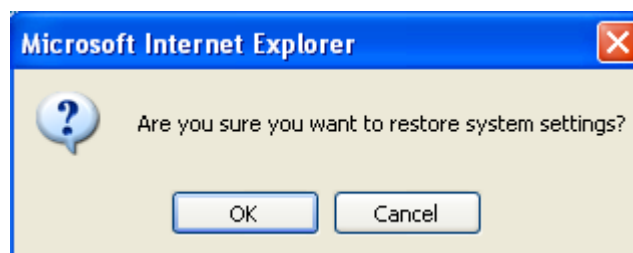
Date / Time	Filename	Configuration		
2014-12-11 00:06:19	MH-2300_system.conf	Download	Restore	Remove
2014-12-11 06:34:26	MH-2300_V2.11.0_20141211.conf	Download	Restore	Remove

Name Settings Help

Company Name : (Max. 63 characters, ex. My Company)

Device Name : (Max. 63 characters, ex. MH-2300)

Resetting the System to Factory Default Settings and Formatting the USB Disk



Confirming to Restore System Settings

2.2.1.4 Enabling Email Notifications

Step 1. Under System > Configuration > Settings, set as shown below:

- Under the **Name Settings** section:
 - Type your company name in the **Company Name** field.
 - Type a name in the **Device Name** field.
- Under the **Email Notification Settings** section:
 - Tick **Enable email notifications**.
 - **Sender Address**: Type a sender address. (Some IPs demand a sender address for email deliveries)
 - **SMTP Server**: Type the IP address of SMTP server.
 - **Email Address 1**: Type the email address of the first recipient.
 - **Email Address 2**: Type the email address of the second recipient.

- Click **OK** at the lower right corner to complete configuration.

Name Settings		Help
Company Name :	MH-2300	(Max. 63 characters, ex. My Company)
Device Name :	MH-2300	(Max. 63 characters, ex. MH-2300)

Email Notification Settings		Help
<input checked="" type="checkbox"/> Enable email notifications		
Sender Address :	inesc@planet.com.tw	(Max. 80 characters, ex. sender@mydomain.com)
SMTP Server :	mail.planet.com.tw	(Max. 80 characters, ex. mydomain.com)
Email Address 1 :	inesc@planet.com.tw	(Max. 80 characters, ex. user1@mydomain.com)
Email Address 2 :		(Max. 80 characters, ex. user2@mydomain.com)
<input type="checkbox"/> Enable SMTP authentication		
Account Name :		(Max. 60 characters)
Password :		(Max. 60 characters)
Email Validity Test :	Send Test	

Enabling the Email Notifications


Test successful.

```

SMTP Se
Sender :
Recipier

Connect to 10.123.123.232
>> 220 mail.planet.com.tw ESMTP SMTPProxy
<< HELO UTM
>> 250 mail.planet.com.tw Hello [10.1.1.248]
<< MAIL FROM: <inesc@planet.com.tw>
>> 250 2.1.0 inesc@planet.com.tw....Sender OK
<< RCPT TO: <inesc@planet.com.tw>
>> 250 2.1.5 inesc@planet.com.tw
<< DATA
>> 354 End data with <CR><LF>.<CR><LF>
<< From: inesc@planet.com.tw
<< To: inesc@planet.com.tw,
<< Subject: Mail Test
<< This is a test message.
<< .

```

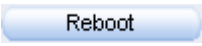
- 

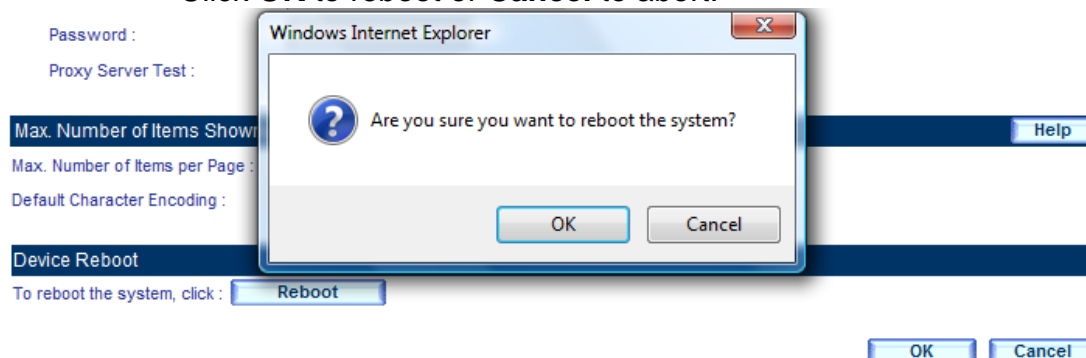
Note

 1. Click the Send Test Mail button to test the validity of email address 1 and 2.
 2. To enable SMTP authentication, tick the box of Enable SMTP authentication and then configure its corresponding settings.

2.2.1.5 Rebooting the MH-2300

Step 1. To reboot the MH-2300, go to **System > Configuration > Settings** and set as shown below:

- Under the **Device Reboot** section, click  at the middle bottom of the screen.
- A confirmation dialogue box appears and asks “Are you sure you want to reboot the system?”
- Click **OK** to reboot or **Cancel** to abort.



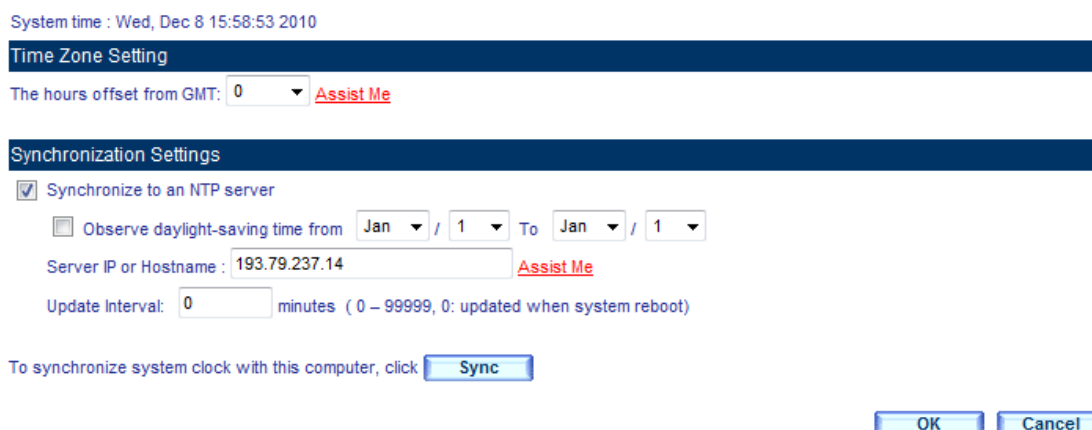
Clicking the Button to Reboot the System

2.2.2 Date / Time

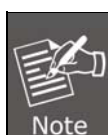
2.2.2.1 Setting the System Clock

Step 2. Under **System > Configuration > Date/Time**, set as shown below:

- Configure the GMT offset.
- Tick the box of **Synchronize to an NTP server**.
- Type the IP address of the Internet time server in the **Server IP or Hostname** field.
- Set an interval time to update system clock.
- Click **OK**.



The System Clock Settings



1. Click **Sync** to synchronize the system clock with that on a local computer.
2. For assistance in configuring GMT offset and NTP sever, click **Assist Me** next to the corresponding setting.

2.2.3 Multiple Subnets

2.2.3.1 Allows Internal Users to Access the Internet via NAT or Routing

Prerequisite Configuration (Note: The IP addresses are used as examples only.)

Configure Port 1 as LAN 1 (192.168.1.1 in NAT Routing mode) to connect it to the LAN subnet 192.168.1.x/24.

Configure Port 2 as WAN 1 (10.10.10.1) and connect it to the ISP router (10.10.10.2); the subnet distributed by the local ISP is 162.172.50.0/24.

Packets traveling to an external network via Port 2 will carry the private IP of 10.10.10.1, which is translated into the mapped address of 162.172.50.1 for signature definition updates.

Configure Port 3 as WAN 2 (211.22.22.22) and connect it to the ADSL Termination Unit Remote (ATUR) to access the Internet.

Step 1. Under **System > Configuration > Multiple Subnets**, set as shown below:

- Specify a name for the subnet.
- **Interface:** Select "Port1 (LAN1)".
- **IP Version:** Select "IPv4".
- **Alias IP Address:** Type "162.172.50.1"
- **Netmask:** Type "255.255.0.0"
- Click **OK**.

Add Subnet

Name : (Max. 30 characters)

Interface : Port1 (LAN1) ▾

IP Version : IPv4 ▾

Alias IP Address : (ex. 192.168.1.1)

Netmask : (ex. 255.255.255.0)

VLAN ID : ☐ Enable VLAN ID (0 - 4095)

Adding a Subnet

/ 1

Name ▲	IP Version	Alias IP Address / Netmask	Interface	VLAN ID	Configuration
subnet_01	IPv4	162.172.50.1 / 255.255.0.0	LAN1		<div style="display: flex; justify-content: space-around;"> <input type="button" value="Modify"/> <input type="button" value="Remove"/> </div>

/ 1

New Entry

Subnet Successfully Added

Note For adding a subnet in a different network, please create corresponding policies for network interconnection, such as LAN-to-LAN or DMZ-to-DMZ. To do so, select "Inside Any" (or DMZ any) for both **Source Address** and **Destination Address**, and then select "Any" for Service when configuring a LAN-to-LAN / DMZ-to-DMZ policy.

Step 2. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to the Port 2.
- For **Interface Type**, select **WAN**, and specify its corresponding network addresses. (refer to your ISP)
- For **NAT Redirection**, select "A designated IP" and then enter "162.172.50.1".

Modify Interface

Interface Designation : WAN1

Interface Type : ☐ Disabled ☒ LAN ☐ WAN ☐ DMZ

Connection Type : ☒ Static IP Address (Leased Line User)
☐ Dynamic IP Address (Cable Modem User)
☐ PPPoE (ADSL Dial-Up User)

IPv4 Settings

IPv4 Address :

Netmask :

IPv4 Default Gateway :

MAC Address :

IPv6 Settings

Connecting using :

IPv6 Address :

Prefix Length :

IPv6 Default Gateway :

Max. Downstream Bandwidth : Mbps (1 - 1000)

Max. Upstream Bandwidth : Mbps (1 - 1000)

Keepalive Properties :

[Help](#) Type :

DNS IP Address :

Domain Name : (Max. 55 characters)

Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection :

[Help](#)

Access by / via : ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[Help](#)

Modifying the WAN Interface

Step 3. Under **Policy Object > Address > LAN**, set as shown below:

Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 1 MB)

[Assist Me](#) ◀ ◻ ▶ / 1 ◻ ◻ ▶

Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		In Use
Lan1_Subnet1	IPv4	All	192.168.1.0 / 255.255.255.255		Modify Remove
Lan1_Subnet2	IPv4	All	162.172.50.0 / 255.255.255.255		Modify Remove

◀ ◻ ▶ / 1 ◻ ◻ ▶

[New Entry](#)

The Address Settings for LAN Subnets

Step 4. Go to **Policy > Outgoing** and configure the following settings:

- Click **New Entry**.
- **Source Address**: Specify a name for the outgoing policy, e.g., "LAN 1_Subnet1".
- **Action**: Tick the box of "Permit all outgoing connections".
- Click **Advanced Settings**.
- Under the **IP Redirection** section, select "Automatic" for **Port 2 (WAN1)** and **Port3 (WAN2)**.
- Click **OK**.
- Click **New Entry**.
- **Source Address**: Specify a name for the outgoing policy, e. g., "LAN 2_Subnet 2".
- **Action**: Tick the box of "Permit all outgoing connections".
- Under the **IP Redirection** section, select "Routing" for **Port 2 (WAN1)** and select "Automatic" for **Port 3 (WAN2)**.
- Click **OK**.

Add Policy

Source Address : Lan1_Subnet1

Destination Address : Outside Any

Service : Any

Schedule : None

Authentication : None

VPN Trunk : None

☐ Permit All ☒ Deny All

Action : Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (Port2)
 ☒ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☒ Enabled

Traffic Grapher : ☒ Enabled

Web Filter : None

Application Blocking : None

Advanced Settings

Creating a Policy to Apply the First LAN Address Settings

Add Policy

Source Address :	Lan1_Subnet2
Destination Address :	Outside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	----- None -----

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

IDP : ☐ Enabled

Anti-Virus :

☐ POP3 ☐ SMTP ☐ HTTP / Web-Based Mail ☐ FTP

Anti-Spam :

☐ POP3 ☐ SMTP

IM Recording : ☐ Enabled

QoS :

----- None -----

Max. Bandwidth Per Source IP :

Downstream Kbps / Upstream Kbps (0: unlimited)

P2P Bandwidth Limits :

Downstream Kbps / Upstream Kbps (0: unlimited)

Max. Concurrent Sessions Per IP :

(1 - 99999, 0: unlimited)

Max. Concurrent Sessions :

(1 - 99999, 0: unlimited)

Traffic Quota per Session :

KB (1 - 999999, 0: unlimited)

Quota Per Source IP :

MB (1 - 999999, 0: unlimited)

Traffic Quota per Day :

MB (1 - 999999, 0: unlimited)

IP Redirection :

Port 1 (LAN1) :	Automatic	<input type="text"/>
Port 2 (WAN1) :	Routing	<input type="text"/>
Port 3 (WAN2) :	Automatic	<input type="text"/>
Port 4 (Port4) :	Automatic	<input type="text"/>

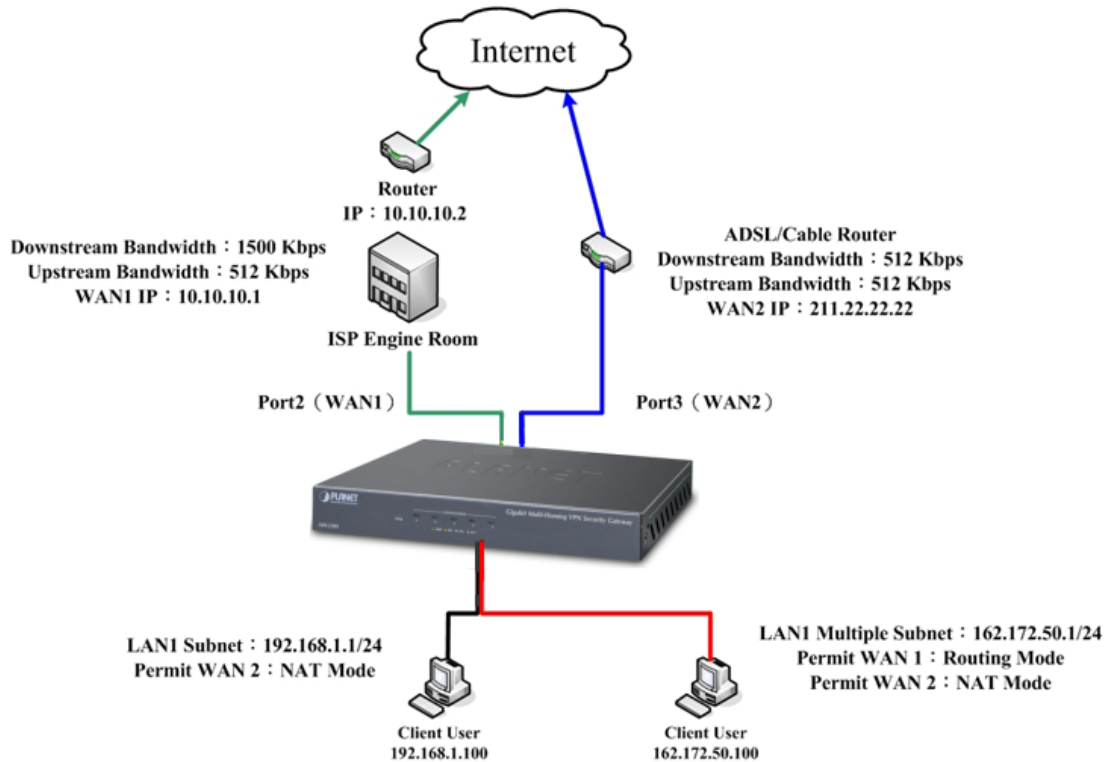
Help

OK


Cancel

Creating a Policy to Apply the Second LAN Address Settings

Step 5. The Internet access for LAN 1 users is illustrated as shown below:



The Deployment of Multiple LAN Subnets to Access the Internet

- | | |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 
Note | <ol style="list-style-type: none"> 1. The subnet 192.168.1.x/24 now can be connected to the Internet through WAN 1/WAN 2 interface via NAT. 2. The subnet 162.172.50.x/24 now can be connected to the Internet through WAN 1 interface via routing or through WAN 2 interface via NAT. |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2.2.4 Routing Table

2.2.4.1 Enabling Two Networks Connected by a Router to Access the Internet via MH-2300

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Company A: Port 1 is defined as LAN 1 (192.168.1.1 in NAT Routing mode) and is connected to the LAN subnet 192.168.1.x/24, which has a subnet 192.168.10.x/24 connected to Router 1 (10.10.10.1 with RIPv2). The LAN interface connected to Router 1 is 192.168.1.252.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Port 3 is defined as WAN 2 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

Company B is using Router 2 (10.10.10.2 with RIPv2) with the subnet 192.168.20.x/24 connected to it.

A leased line connects Company A's Router 1 (10.10.10.1) with Company B's

Router 2 (10.10.10.2).

Step 1. Go to **System > Configuration > Routing Table** and then set as shown below:

- Click **New Entry**.
- **IP Version** : Select "IPv4".
- **IP Address**: Type "192.168.10.0".
- **Netmask**: "255.255.255.0".
- **Gateway** : "192.168.1.252".
- **Interface** : Select "Port 1 (LAN1)".
- Click **OK**.
- Click **New Entry**.
- **IP Version** : Select "IPv4".
- **IP Address**: Type "192.168.20.0".
- **Netmask**: "255.255.255.0".
- **Gateway** : "192.168.1.252".
- **Interface** : "Port1 (LAN1)".
- Click **OK**.
- Click **New Entry**.
- **IP Version** : Select "IPv4".
- **IP Address**: Type "10.10.10.0".
- **Netmask**: Type "255.255.255.0".
- **Gateway** : Type "192.168.1.252".
- **Interface** : Select " Port1 (LAN1)".
- Click **OK**.

Add Static Routing Address	
IP Version :	IPv4 ▼
IP Address :	192.168.10.0 (ex. 192.168.100.1)
Netmask :	255.255.255.255 (ex. 255.255.255.255)
Gateway :	192.168.1.252 (ex. 192.168.1.10)
Interface :	Port1 (LAN1) ▼

OK **Cancel**

Adding the First Static Routing Address

Add Static Routing Address	
IP Version :	IPv4 ▼
IP Address :	192.168.20.0 (ex. 192.168.100.1)
Netmask :	255.255.255.255 (ex. 255.255.255.255)
Gateway :	192.168.1.252 (ex. 192.168.1.10)
Interface :	Port1 (LAN1) ▼

OK **Cancel**

Adding the Second Static Routing Address


Add Static Routing Address

IP Version :	IPv4 ▾	
IP Address :	10.10.10.0	(ex. 192.168.100.1)
Netmask :	255.255.255.255	(ex. 255.255.255.255)
Gateway :	192.168.1.252	(ex. 192.168.1.10)
Interface :	Port1 (LAN1) ▾	

Adding the Third Static Routing Address

Static Routing					
IP Version	Destination IP / Netmask(Prefix Length)	Gateway	Interface	Configuration	
IPv4	192.168.10.0 / 255.255.255.255	192.168.1.252	LAN1	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
IPv4	192.168.20.0 / 255.255.255.255	192.168.1.252	LAN1	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
IPv4	10.10.10.0 / 255.255.255.255	192.168.1.252	LAN1	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

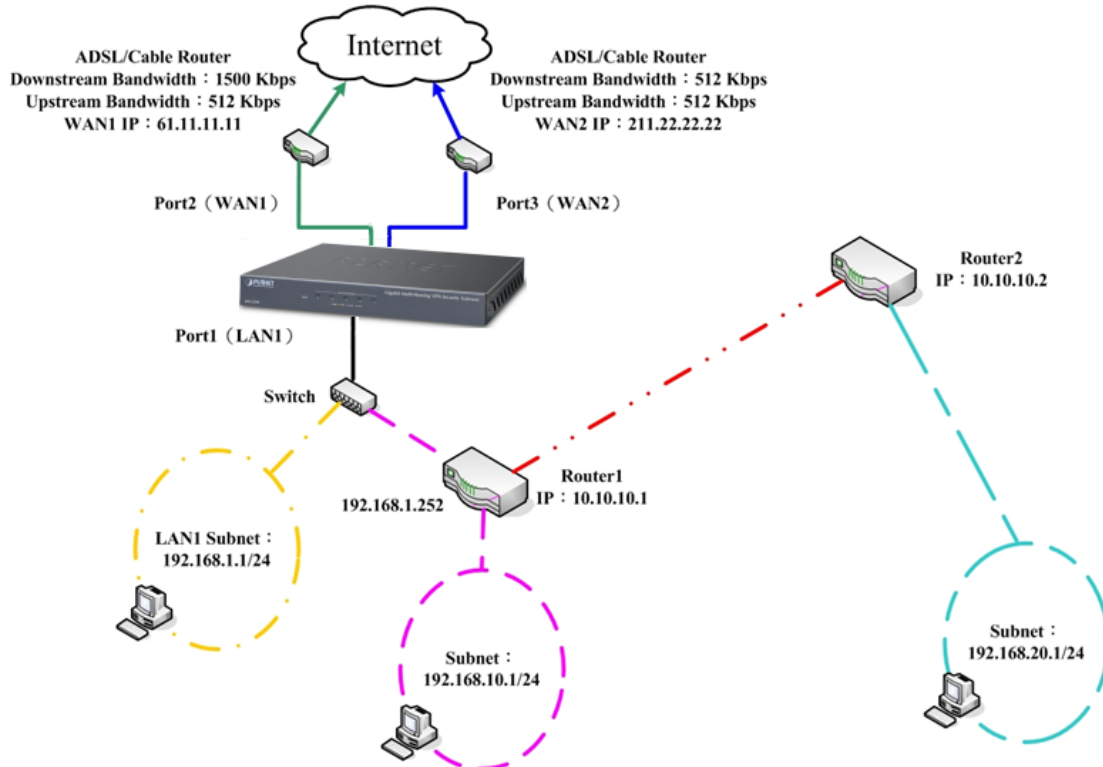
Static Routing Addresses Successfully Added



Note

For adding a subnet in a different network, please create corresponding policies for network interconnection, such as LAN-to-LAN or DMZ-to-DMZ. To do so, select "Inside Any" (or DMZ any) for both **Source Address** and **Destination Address**, and then select "Any" for Service when configuring a LAN-to-LAN / DMZ-to-DMZ policy.

Step 2. The LAN subnets of 192.168.10.x/24, 192.168.20.x/24 and 192.168.1.x/24 are interconnected and are connected to the Internet through MH-2300 via NAT.



The Deployment of Multiple LAN Subnets to Access the Internet via Routing

2.2.5 DHCP

2.2.5.1 Automatically Allocating IP Addresses to LAN PCs

Step 1. Go to **System > Configuration > DHCP** and then set as shown below:

- Select the radio box of "Enable DHCP".
- Untick the box of "Obtain DNS server address automatically".
- **IPv4 DNS Server 1:** Type an IP as the primary DNS Server.
- **IPv4 DNS Server 2:** Type an IP as the secondary DNS Server.
- **IPv4 WINS Server 1:** Type an IP as the primary WINS Server.
- **IPv4 WINS Server 2:** Type an IP as the secondary WINS Server.
- **Lease Time :**Type a lease time for the allocated IP addresses (24 hours by default).
- Configure the following settings based on your LAN or DMZ subnet:
 - ◆ **IPv4 Range 1 :** Specify the first range of the IP pool (must be within the same subnet). By default, it is between 192.168.1.2 and 192.168.1.254.
 - ◆ **IPv4 Range 2:** Specify the second range of the IP pool (must be within the same subnet and not repeated from those in the first range).

- Click **OK**.

DHCP Settings

☐ Disable DHCP
☒ Enable DHCP

Domain Name : (Max. 80 characters)

☐ Obtain DNS server address automatically

IPv4 DNS Server 1 :
 IPv4 DNS Server 2 :
 IPv6 DNS Server 1 :
 IPv6 DNS Server 2 :
 IPv4 WINS Server 1 :
 IPv4 WINS Server 2 :
 IPv6 WINS Server 1 :
 IPv6 WINS Server 2 :

Leased Time : hour(s) (1 - 99999)

Static IP Assignment : [Assign Static IP](#)

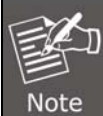
☒ LAN1

- ☒ IPv4
 - IPv4 Range 1 : -
 - IPv4 Range 2 : -
- ☐ IPv6
 - IPv6 Range 1 : -
 - IPv6 Range 2 : -

☒ LAN2

- ☒ IPv4
 - IPv4 Range 1 : -
 - IPv4 Range 2 : -
- ☐ IPv6
 - IPv6 Range 1 : -
 - IPv6 Range 2 : -

Configuring the DHCP Server to Automatically Distribute IP Addresses



When the box of "Obtain DNS server address automatically" is ticked, the primary DNS server on LAN PCs will be defaulted to MH-2300's LAN interface address. This feature is recommended for the Internet access through a local authentication. (Users are redirected to the authentication screen for the attempt to access the Internet.)

2.2.5.2 Manually Allocating an IP Address to a LAN PC

Step 1. Under **System > Configuration > DHCP**, set as shown below:

- Click [Assign Static IP](#)
- Click **New Entry**.


- From the drop-down list, select the **Interface** and **IP Version** based on the LAN user, respectively.
- Specify the IP address and MAC address in the corresponding fields.
- Click **OK** to complete the settings.

Add New Static IP Address

Interface :	LAN1 ▼								
IP Address :	192.168.1.2	(ex. 192.168.1.10)							
MAC Address :	A8:F7:E0:11:22:33	Clone MAC Address							

[OK](#)
[Cancel](#)

Configuring the DHCP Server to Distribute an IP Address



Note

1. For the convenience of configuration, the MAC address is also obtainable by clicking the **Clone MAC Address** button.
2. The DHCP-distributed IP addresses listed under **System > Configuration > DHCP** are available for export and import. The IP addresses may be exported for editing and archival purposes and imported in the event of data loss.

2.2.6 Dynamic DNS

Step 1. Go to **System > Configuration > Dynamic DNS** and then set as shown below:

- Click **New Entry**.
- Select a **Service Provider** from the drop-down list.
- Tick the box of “Use the IP of” and then select a WAN port from the drop-down list.
- Type your **Username**, **Password** and **Domain Name** based on your DDNS service.
- Click **OK**.

Add Dynamic DNS

Service Provider :	DynDNS (www.dyndns.com) [U.S.A.] ▼								
Real IP Address :	203.73.55.229	<input checked="" type="checkbox"/> Use the IP of	Port 4 (WAN1) ▼						
Username :	albert180	(Max. 60 characters)							
Password :	••••••	(Max. 60 characters)							
Domain Name :	albert180	dyndns.org ▼	(Max. 80 characters)						


[OK](#)
[Cancel](#)

Configuring the Dynamic DNS Settings

Help			
Connection	Domain Name ▲	Real IP Address	Configuration
	albert180.dyndns.org	203.73.55.229	<div>Modify</div> <div>Remove</div>




New Entry

Dynamic DNS Settings Successfully Added



Note

- The description of the symbols used in Dynamic DNS are as follows:

Symbol			
Description	Connection Successful	Connection Failed	Connected
- If you do not have a Dynamic DNS account, you may select a service provider from the drop-down list and then click **Sign up** next to it to register an account.
- The **Real IP Address** can be specified by either ticking the box of "Use the IP of" or simply entering the address in the field.

2.2.7 Host Table

Step 1. Go to **System > Configuration > Host Table** and then set as shown below:

- Click **New Entry**.
- **Hostname**: Specify a name for the host.
- **IP Version**: Select "IPv4".
- **IP Address**: Type the private IP address that the host is mapped to.
- Click **OK**.

Add Hostname

Hostname : (Max. 80 characters, ex. www.my_domain.com)


IP Version :

IP Address : (ex. 192.168.1.10)

OK

Cancel

Adding a Hostname



Note

Host Table requires the **Preferred DNS server** on the local PCs to be specified as the same as the LAN or DMZ interface address to be effective. For further information on configuring **Preferred DNS server**, please refer to: <http://windows.microsoft.com/en-US/windows-vista/Change-TCP-IP-settings>

2.2.8 Language

2.2.8.1 Switching the System Language

Step 1. Under **System > Configuration > Language**, you may switch the language of the user interface.



Management Interface Language Selection

☒ English

☐ 繁體中文

☐ 简体中文

OK Cancel

[The Language Settings](#)

Chapter 3. Interface

3.1 Interface

This chapter will cover the configuration of network interfaces as well as their connection methods. The interfaces are allowed for defining as different network types (LAN, WAN and DMZ) and being grouped together according to your topology plan, which helps assist in network management.

Terms in Settings

DNS Settings

- Assign the DNS servers for domain name resolution.

MTU Setting

- The Maximum Transmission Unit (MTU) controls the maximum buffer size used for inter-node communication in bytes. By default, it is 1500 bytes.

Incoming Packet Header Logging

- When enabled, packets destined to or originated from MH-2300 are logged in details, which are available under **Monitoring > Logs > Traffic**.

Terms in Interface

Load Balancing Mode

- **Auto**: Distributes sessions according to the utilization of each NIC port, perfectly suited for multiple WAN links at different speeds.
- **Round-Robin**: Distributes sessions across NIC ports at a one-to-one ratio, perfectly suited for multiple WAN links at the same speed.
- **By Traffic**: Distributes sessions by the total traffic processed by each NIC port.
- **By Session**: Distributes sessions based on the saturation threshold of each NIC port.
- **By Packet**: Distributes sessions based on the total packets processed by each NIC port.
- **By Source IP**: Distributes sessions over the same NIC ports for services that requires IP persistence, such as gaming and banking.
- **By Destination IP**: Distributes sessions over the NIC port that a server session was last initiated.

Port

- The sequential number of a physical port.

Interface Designation

- The system-assigned name based on the selected interface type.

Interface Type

- The network interface is categorized into four types:
 - ◆ Local Area Network (LAN)
 - ◆ Wide Area Network (WAN)
 - ◆ Demilitarized Zone (DMZ)

LAN Connection Type (only configurable for WANs)

- It has three connection types, namely:
 - ◆ **NAT Routing:** Allows private IP addresses (available and valid ones) to be translated into public addresses based on network policy.
 - ◆ **Transparent Bridging:** Allows internal users to access a specific networking device in a different network based on network policy through the default gateway. Note: This type requires configuring **Interface Group** settings under **Network**.
 - ◆ **Transparent Routing:** Provides internal users with direct access to the Internet due to being in the same subnet range.

IPv4 Settings

- Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and it is by far the most widely deployed Internet Layer protocol.
- IPv4 addresses are written in dot-decimal notation, which consists of the four octets of the address expressed in decimal and separated by periods, such as 192.168.1.1.
- Please configure the **IPv4 Address**, **Netmask** and **MAC Address** fields according to your network addresses.

IPv6 Settings


- Internet Protocol version 6 (IPv6) is called the “IP Next Generation” (IPng), which is designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. It is backward compatible and thus expected to slowly replace IPv4, with the two existing side by side for many years.
- IPv6 address represent itself as text string using the following three conventional forms:
 - ◆ **Colon-hexadecimal form:** This is the preferred form n:n:n:n:n:n:n:n. Each n represents the hexadecimal value of one of the eight 16-bit elements of the address. For example:
21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
 - ◆ **Compressed form:** It is used to simplify writing addresses that contains a long string of zeros, use the compressed form, in which a single contiguous sequence of 0 blocks are represented by a double-colon symbol (::). This symbol can appear only once in an address. For example, the unicast address FE80:0:0:0:2AA: FF: FE9A:4CA2 in compressed form is FE80:: 2AA:FF:FE9A:4CA2.
 - ◆ **Mixed form:**
 - **IPv4-compatible addresses:** The IPv4-compatible address, 0:0:0:0:0:0:w.x.y.z or ::w.x.y.z (where w.x.y.z is the dotted decimal

representation of a public IPv4 address), is used by IPv6/IPv4 nodes that are communicating with IPv6 over an IPv4 infrastructure. When the IPv4-compatible address is used as an IPv6 destination, the IPv6 traffic is automatically encapsulated with an IPv4 header and sent to the destination using the IPv4 infrastructure.

- **IPv4-mapped addresses:** The IPv4-mapped address, 0:0:0:0:FFFF:w.x.y.z or ::FFFF:w.x.y.z, represents an IPv4-only node to an IPv6 node. For example, ::ffff:192.0.2.128 is the IPv4-mapped IPv6 address for IPv4 address 192.0.2.128.
- The leading bits in the address define the specific IPv6 address type. The variable-length field containing these leading bits is called a Format Prefix (FP). An IPv6 unicast address is divided into two parts. The first part contains the address prefix (also known as subnet prefix such as 21DA:D3:0:2F3B::/64), and the second part contains the interface identifier (MAC address).
 - ◆ A concise way to express an IPv6 address/prefix combination is as follows: ipv6-address/prefix-length. For example, an IPv6 address with a 64-bit prefix is represented as 3FFE:FFFF:0:CD30:0:0:0:0/64 or compressed as 3FFE:FFFF:0:CD30::/64.
 - ◆ Although prefixes can be defined along bit boundaries, the colon hexadecimal notation for IPv6 addresses is expressed along nibble (4-bit) boundaries. To properly express a subnet with a prefix where its prefix length is not a multiple of 4, you must complete hexadecimal to binary conversions to determine the appropriate subnet identifier. For example, to express the subnet of the address and prefix of 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/59, you must convert the “3” in “2F3B” to binary (0011), divide the nibble between the third and fourth binary digits, and then convert back to hexadecimal. The result is the subnet identifier of 21DA:D3:0:2F20::/59.
- IPv6 address is classified into three types:
 - ◆ **Unicast address:**
 - **Link-local addresses:** These addresses are used on a single link and have the following format: FE80::InterfaceID. Link-local addresses are used primarily at startup and when the system has not yet acquired addresses of larger scope. They are analogous to IPv4's RFC 3927 addresses (169.254.0.0/16).
 - **Site-local addresses:** These addresses are used on a single site and have the following format: FEC0::SubnetID:InterfaceID. The site-local addresses are used for addressing inside a site without the need for a global prefix. They are analogous to IPv4's RFC1918 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).
 - **Global IPv6 unicast addresses:** These addresses can be used across the Internet and have the following format: 010 (FP, 3 bits) TLA ID (13 bits) Reserved (8 bits) NLA ID (24 bits) SLA ID (16 bits) InterfaceID (64 bits).
 - ◆ **Multicast address:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to this address is delivered

to all the interfaces identified by the address. The multicast address types supersede the IPv4 broadcast addresses. They are prefixed with FF (that is, the first bits are 11111111) such as FF02::1 for all nodes address, FF02::2 for all routers address, etc.

- ◆ **Anycast address:** An identifier for a set of interfaces (typically belonging to different nodes). A packet sent to this address is delivered to only one interface identified by the address. This is the nearest interface as identified by routing metrics.



Converting an MAC address (00-AA-00-3F-2A-1C) to EUI-64 format:


- FF-FE is inserted between the third and fourth bytes. This yields 00-AA-00-FF-FE-3F-2A-1C.
- The U/L bit, which is the seventh bit in the first byte, is complemented. The first byte in binary form is 00000000. When the seventh bit is complemented, it becomes 00000010 (0x02).
- The result, 02-AA-00-FF-FE-3F-2A-1C, is converted to colon-hexadecimal notation, yielding the interface identifier 2AA:FF:FE3F:2A1C. Thus, in this example, the link-local address that corresponds to the network adapter with the MAC address of 00-AA-00-3F-2A-1C is FE80::2AA:FF:FE3F:2A1C.

MAC Address


- Configure the MAC address accordingly.

Any IP Routing

- When enabled, no network configuration (IP address, netmask, default gateway, DNS settings, etc.) is required for users to access the Internet.
- Saves the hassle of configuring network settings for both users and the administrator.



1. For hoteliers (hotel, inn, B&B, etc.) to provide customers with Internet service.
2. This feature is not intended for an office scenario. There could be an IP conflict issue due to the same LAN IP address.



Any IP Routing is subject to and only configurable for LAN interfaces.

Ping / Tracert

- When ticked, the network can be detected by ping/tracert command.

HTTP

- When ticked, the management interface is available for access via HTTP protocol.

HTTPS

- When ticked, the management interface is available for access via HTTPS protocol.

Telnet

- When ticked, the management interface is available for access via Telnet protocol.

SSH

- When ticked, the management interface is available for access via SSH protocol.

WAN Connection Type (only configurable for WAN)

- There are three connection types:
 - ◆ Static IP Address (Leased Line User)
 - ◆ Dynamic IP Address (Cable Modem User)
 - ◆ PPPoE (ADSL Dial-up User)

Keepalive Properties Type

- The two verification methods for Internet availability are listed as follows:
 - ◆ **ICMP**: Verifies the Internet availability by pinging a specific IP address.
 - ◆ **DNS**: Verifies the Internet availability by requesting a specific domain name.

NAT Redirection

- Translates private IP addresses into public addresses.
 - ◆ **Auto-configuration**: The public address is automatically designated to the IP address of an active WAN link.
 - ◆ **A designated IP**: The public address is manually designated to the IP address of an available WAN link.

Max. Downstream & Upstream Bandwidth

- Specify a proper bandwidth separately for downstream and upstream operations.

Disconnect if idle for...minutes

- Specify an idle timeout to automatically disconnect the Internet via PPPoE dial-up connection. Type "0" to stay connected or a value from 1 to 99,999 (time unit: minute) for disconnection.

DMZ Connection Type (only configurable for DMZ)

- Please refer to "**LAN Connection Type**".

Saturated Connections

- Determines the maximum sessions allowed for each WAN interface when running in **By Traffic**, **By Session** or **By Packet** mode. New sessions will be distributed to other WAN interfaces when the value has been exceeded

Priority

- The priority of a WAN interface in the connectivity.

Terms in Interface Group

Interface Group

- Allows for physically isolating network interfaces by NIC teaming. The feature is intended for a scenario that runs in Transparent Bridging mode and accesses the Internet via a static IP.
- Allows for translating private addresses (LAN or DMZ) to a public address when running in Transparent Bridging mode.

3.1.1 Examples of Interface

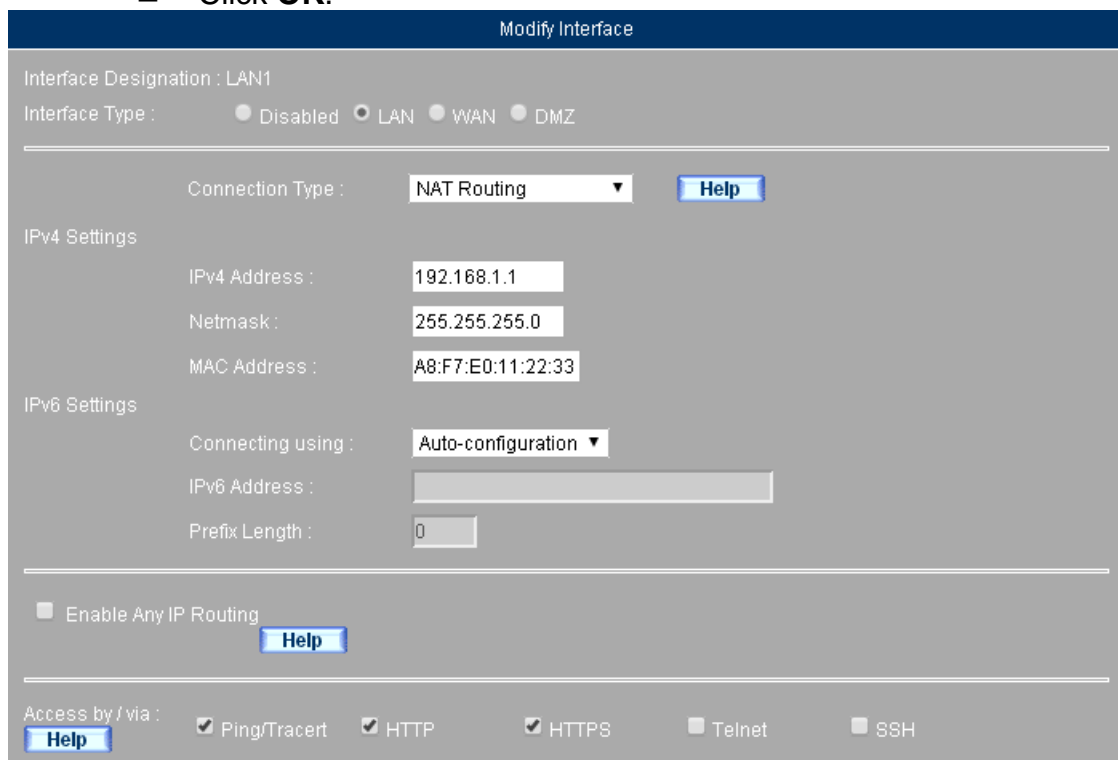
3.1.1.1 Modifying the LAN Interface (in NAT Routing Mode)

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Configure Port 1 as LAN 1 (192.168.1.1 in NAT Routing mode)


Step 1. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to Port 1.
- Select “LAN” for **Interface Type**.
- Select “NAT Routing” for **Connection Type**.
- Specify the **IPv4 Address** and **Netmask**.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.



OK Cancel

Modifying the LAN Interface Settings

- 
Note

1. The LAN subnet is defaulted and subject to "192.168.1.x/24". Therefore, the access to the management interface requires an IP address from the same subnet
 2. The management interface may not be accessible once the boxes of **HTTP** and **HTTPS** are unticked prior to the configuration of permitted IP under **System > Administration**.

3.1.1.2 Configuring the WAN Interface

Step 1. Under **Network > Interface**, click **Modify** corresponding to Port 2 and select **WAN** for **Interface Type**.

Step 2. Configure the **Keepalive Properties** as follows:

- If "ICMP" is selected as the type, then enter the **Alive Indicator Site IP**.
- If "DNS" is selected as the type, then enter the **DNS IP Address** and the **Domain Name**.
- Enter the **Minimum Interval**.

Keepalive Properties :

Type : ICMP

Alive Indicator Site IP : 168.95.1.1

Minimum Interval : 5 second(s) (0 - 99, 0: no detection)

Keepalive Detection Using ICMP

Keepalive Properties :


Type : DNS

DNS IP Address : 168.95.1.1

Domain Name : www.hinet.net (Max. 55 characters)

Minimum Interval : 5 second(s) (0 - 99, 0: no detection)

Keepalive Detection Using DNS

- 
Note

Keepalive Properties is used for network connectivity detection. Consequently, the accuracy of detection is subject to the availability of **Alive Indicator Site IP**, **DNS IP Address** and **Domain Name**.

Step 3. Configure the **Interface Type** as follows:

- When connecting using **Static IP Address**:
 - ◆ Enter the **IP Address**, **Netmask** and **Default Gateway**.
 - ◆ Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth**.
 - ◆ Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
 - ◆ Click **OK**.
- When connecting using **Dynamic IP Address (Cable Modem User)**:
 - ◆ Click **Renew** to obtain an IP address automatically.

- ◆ Click the **Clone MAC Address** button to obtain the MAC Address.
- ◆ Enter the **Username** provided by the ISP.
- ◆ Enter the **Domain Name** provided by the ISP.
- ◆ Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth**.
- ◆ Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- ◆ Click **OK**.
- **When connecting using PPPoE (ADSL Dial-Up User):**
 - ◆ Enter the **Account Name** for the connection.
 - ◆ Enter the **Password** for the connection.
 - ◆ **IP Address Obtained from ISP Via:** Select "Dynamic".
 - ◆ Enter the **Max. Downstream Bandwidth** and the **Max. Upstream Bandwidth**.
 - ◆ Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
 - ◆ Click **OK**.

Modify Interface

Interface Designation : WAN1

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☒ Static IP Address (Leased Line User)

☐ Dynamic IP Address (Cable Modem User)

☐ PPPoE (ADSL Dial-Up User)

IPv4 Settings

IPv4 Address :

Netmask :

IPv4 Default Gateway :

MAC Address :

IPv6 Settings

Connecting using :

IPv6 Address :

Prefix Length :

IPv6 Default Gateway :

Max. Downstream Bandwidth : Kbps (1 - 512000)

Max. Upstream Bandwidth : Kbps (1 - 512000)

Keepalive Properties :

[Help](#) Type :

Alive Indicator Site IP :

Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection :

[Help](#)

Access by / via :

[Help](#) ☒ Ping ☒ HTTP ☒ HTTPS ☒ Telnet ☒ SSH

Configuring the Static IP Connection Settings

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.10.1 / 255.255.255.0	--- ▼	Modify	--- ▼
2	DMZ1	NAT Routing	192.168.2.1 / 255.255.255.0	--- ▼	Modify	--- ▼
3	WAN2	Static IP	61.62.236.15 / 255.255.255.0	--- ▼	Modify	1 ▼
4	WAN1	PPPoE	203.73.55.229 / 255.255.255.255	--- ▼	Modify	2 ▼

Static IP Connection Settings Successfully Completed

Modify Interface

Interface Designation : WAN2

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☐ Static IP Address (Leased Line User)
☒ Dynamic IP Address (Cable Modem User)
☐ PPPoE (ADSL Dial-Up User)

IP Address : 0.0.0.0 Renew Release

Netmask : 0.0.0.0

MAC Address : A8:F7:E0:11:22:33 Clone MAC

Username : (Max. 50 characters)

Domain Name : (Max. 80 characters)

Max. Downstream Bandwidth : 0 Mbps (1 - 1000)

Max. Upstream Bandwidth : 0 Mbps (1 - 1000)

Keepalive Properties :

Help Type : DNS ▼

DNS IP Address : 168.95.1.1

Domain Name : www.hinet.net (Max. 55 characters)

Minimum Interval : 5 second(s) (0 - 99, 0: no detection)

NAT Redirection : A designated IP ▼ 162.172.50.1

Help

Access by / via : ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

Help

Configuring the Dynamic IP Connection Settings

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.10.1 / 255.255.255.0	--- ▼	Modify	--- ▼
2	DMZ1	NAT Routing	192.168.2.1 / 255.255.255.0	--- ▼	Modify	--- ▼
3	WAN2	Static IP	61.62.236.15 / 255.255.255.0	--- ▼	Modify	1 ▼
4	WAN1	Dynamic IP	203.73.66.63 / 255.255.255.255	--- ▼	Modify	2 ▼

Dynamic IP Connection Settings Successfully Completed

Modify Interface

Interface Designation : WAN2

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☐ Static IP Address (Leased Line User)
☐ Dynamic IP Address (Cable Modem User)
☒ PPPoE (ADSL Dial-Up User)

Current Status : Disconnected [Connect](#) [Disconnect](#)

IP Address : 0.0.0.0

Netmask : 0.0.0.0

Account Name :

Password :

IP Address Obtained from ISP Via : ☒ Dynamic ☐ Static

IP Address :
 Netmask :
 Default Gateway :

Disconnect if idle for: minutes (0 - 99999, 0: stays connected)

Max. Downstream Bandwidth : Kbps (1 - 512000)

Max. Upstream Bandwidth : Kbps (1 - 512000)

Keepalive Properties :

[Help](#) Type : DNS

DNS IP Address :

Domain Name : (Max. 55 characters)

Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection : Auto-configuration

[Help](#)

Access by / via : ☒ Ping ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[Help](#)

Configuring the PPPoE Connection Settings

Load Balancing Mode : Auto ("Auto" is recommended)

Port	Name	Connection Type	IP Address / Netmask	Saturated Connections	Configuration	Priority
1	LAN1	NAT Routing	192.168.10.1 / 255.255.255.0	<div><div></div></div>	Modify	<div><div></div></div>
2	DMZ1	NAT Routing	192.168.2.1 / 255.255.255.0	<div><div></div></div>	Modify	<div><div></div></div>
3	WAN2	Static IP	61.62.236.15 / 255.255.255.0	<div><div></div></div>	Modify	<div><div>1</div></div>
4	WAN1	PPPoE	61.59.236.42 / 255.255.255.255	<div><div></div></div>	Modify	<div><div>2</div></div>

PPPoE Connection Settings Successfully Completed



1. The DNS server is configurable under **Network > Settings**.
2. The management interface is accessible externally (by diagnostic commands or web browsers) only if the Ping / Tracert, HTTP, HTTPS, Telnet and SSH settings from a WAN interface are enabled. Nevertheless, it is not recommended to allow external access to the system via these services due to the security concerns. If it is necessary to do so, then only permit the access to

the specific users by their IP address under **System > Administration > Permitted IPs.**

3.1.1.3 Using MH-2300 as a Gateway to Manage the Internet Access to Two LAN Subnets via NAT Routing Mode

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Configure Port1 as WAN1 (61.11.11.11) and connect it to the ADSL modem (ATUR) to access the Internet.

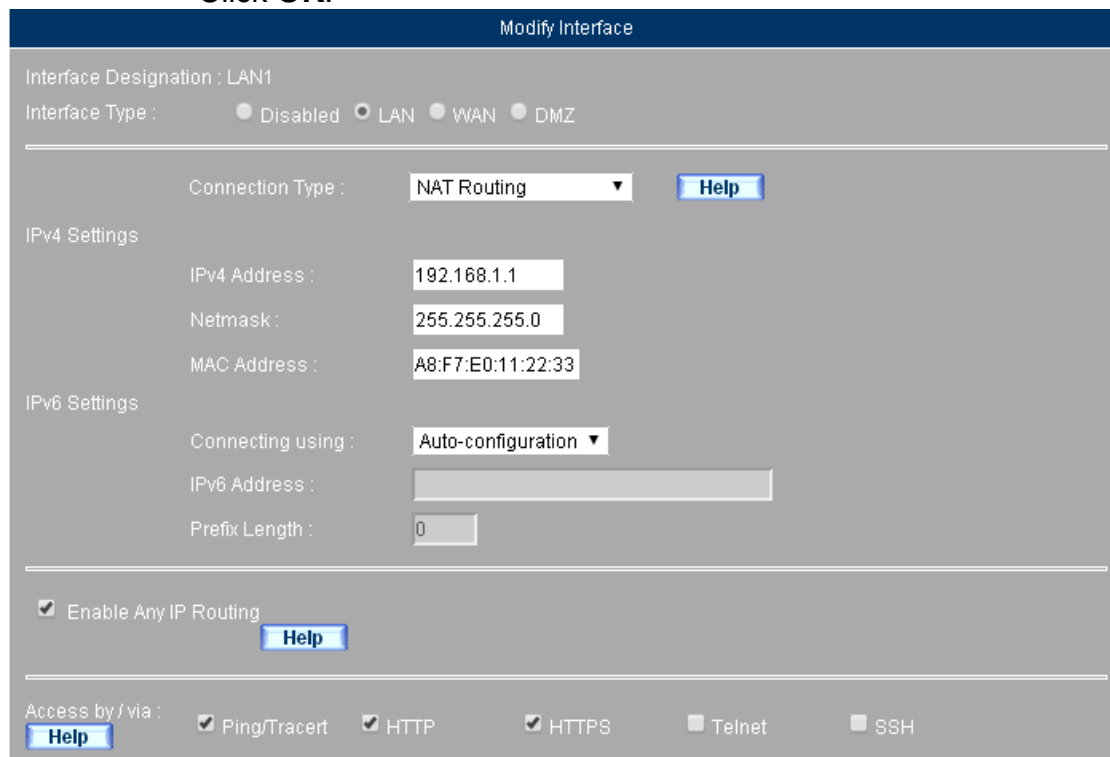
Configure Port2 as LAN1 (192.168.1.1 in NAT Routing mode) and connect it to the LAN subnet 192.168.20.x/24, which is translated to 61.11.11.11 (WAN1) for providing LAN users with Internet access.

Configure Port3 as LAN2 (192.168.2.1 in NAT Routing mode) to connect it to the LAN subnet 192.168.2.x/24, which is translated to 61.11.11.11 (WAN1) for providing LAN users with Internet access.

The two LAN subnets are interconnected through network policies.

Step 1. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 2.
- Select “LAN” for **Interface Type**.
- Select “NAT Routing” for **Connection Type**.
- Specify the **IPv4 Address** and **Netmask**.
- Tick the boxes of “Ping/Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.

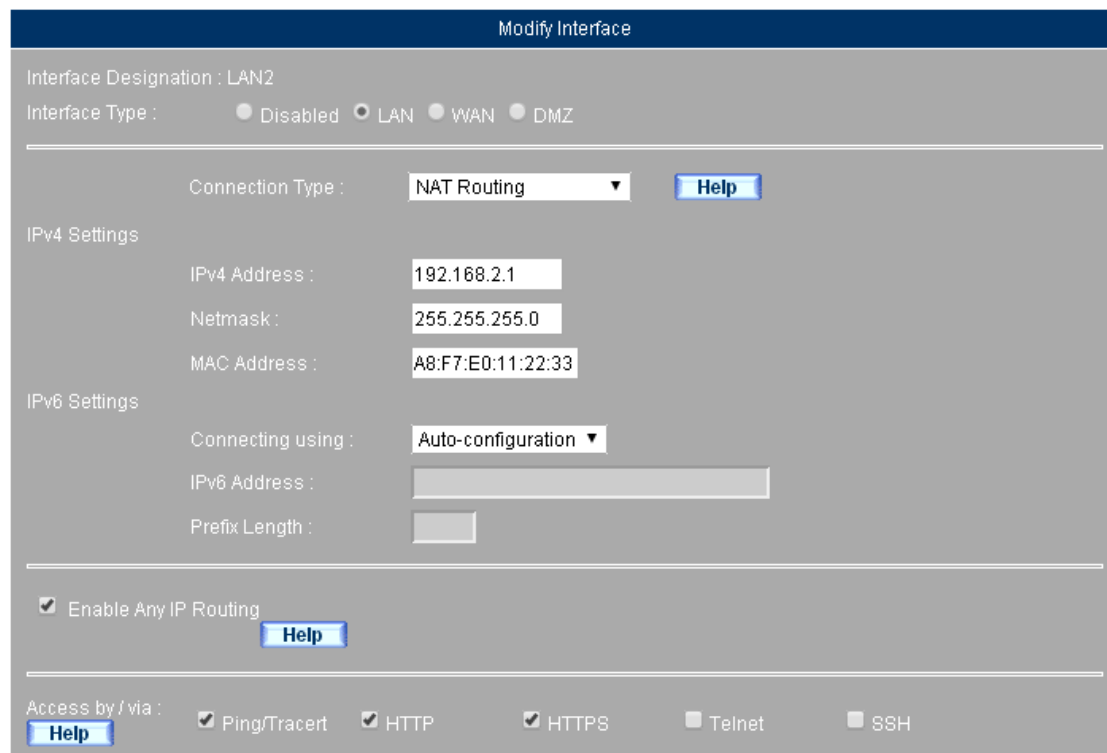


OK Cancel

Modifying the LAN Interface Settings

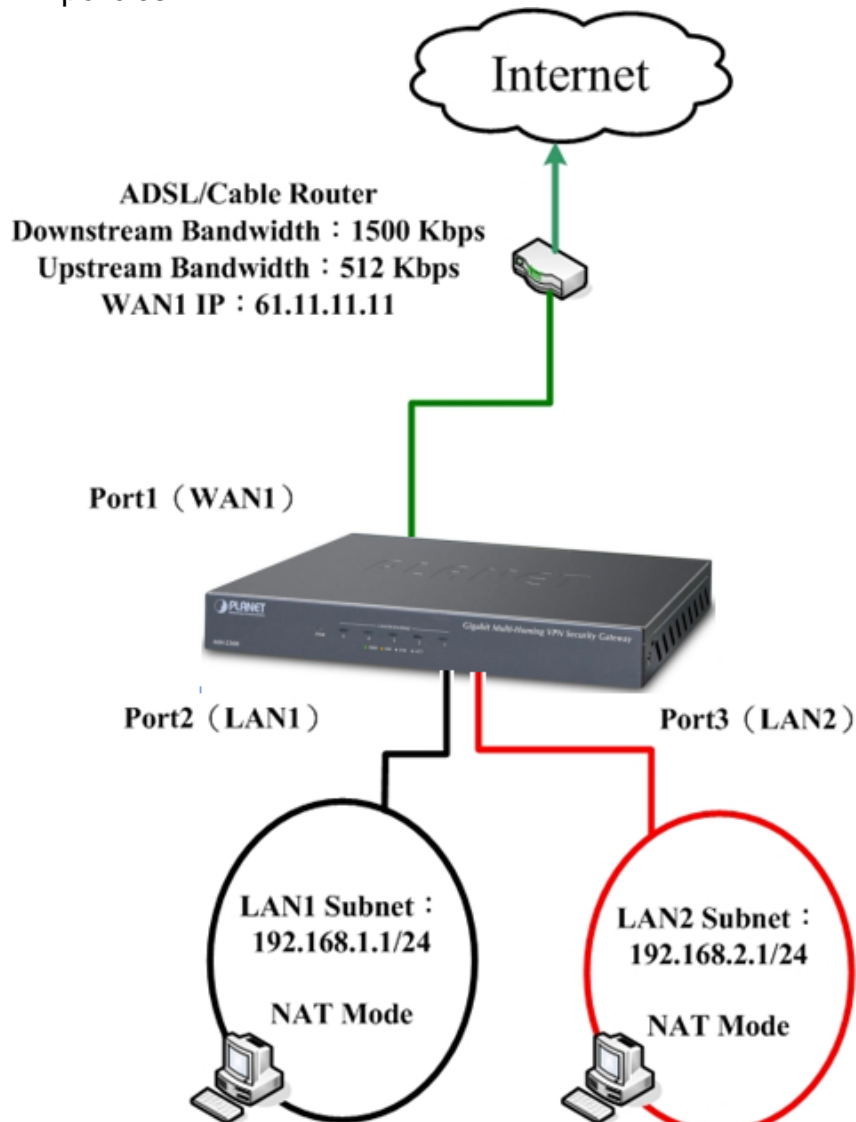
Step 2. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port3.
- Select "LAN" for **Interface Type**.
- Select "NAT Routing" for **Connection Type**.
- Enter the **IPv4 Address** and the **Netmask**.
- Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- Click **OK**.



Modifying the LAN Interface Settings

Step 3. The LAN subnets are now connected to the Internet through WAN 1 (61.11.11.11) via NAT Routing and interconnected through network policies.



The Deployment of Two NAT-routed LAN Subnets

3.1.1.4 Deploying MH-2300 between a Gateway and Two LAN Subnets (Separately Running in Transparent Routing and NAT Routing Modes) to Manage the Internet Access of Internal Users

Prerequisite Configuration (Note: IP addresses are used as examples only)

On the existing firewall, specify two LAN subnets, namely 192.168.1.x/24 (with the gateway set to 192.168.1.1) and 192.168.2.x/24 (with the gateway set to 192.168.2.1)

Configure Port1 as WAN1(192.168.1.2) and connect it to the gateway

(192.168.1.1).

Specify a static route from 192.168.2.x/24 to 192.168.1.2 (WAN 1).

Configure Port2 as LAN1 (Transparent Routing mode) and connect it to the LAN subnet 192.168.1.x/24 (with the gateway set to 192.168.1.1) for providing LAN users with Internet access.

Configure Port3 as LAN2 (192.168.2.1 in NAT Routing mode to connect it to the LAN subnet 192.168.2.x/24 for providing LAN users with Internet access (with the gateway set to 192.168.2.1). LAN PCs may use the original IP to access the Internet.

The two LAN subnets are interconnected through network policies.

Step 1. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 2.
- Select "LAN" for **Interface Type**.
- Select "Transparent Routing" for **Connection Type**.
- Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- Click **OK**.

Modify Interface

Interface Designation : DMZ1

Interface Type : ☐ Disabled ☐ LAN ☐ WAN ☒ DMZ

Connection Type : Transparent Bridging Help

Access by / via : Help ☒ Ping ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

OK Cancel

Configuring the LAN Interface Settings

Step 2. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port3.
- Select "LAN" for **Interface Type**.
- Select "NAT Routing" for **Connection Type**.
- Enter the **IPv4 Address** and the **Netmask**.
- Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- Click **OK**.

Modify Interface

Interface Designation : LAN2

Interface Type : ☐ Disabled ☒ LAN ☐ WAN ☐ DMZ

Connection Type : NAT Routing Help

IPv4 Settings

IPv4 Address : 192.168.2.1

Netmask : 255.255.255.0

MAC Address : A8:F7:E0:11:22:33

IPv6 Settings

Connecting using : Auto-configuration

IPv6 Address :

Prefix Length :

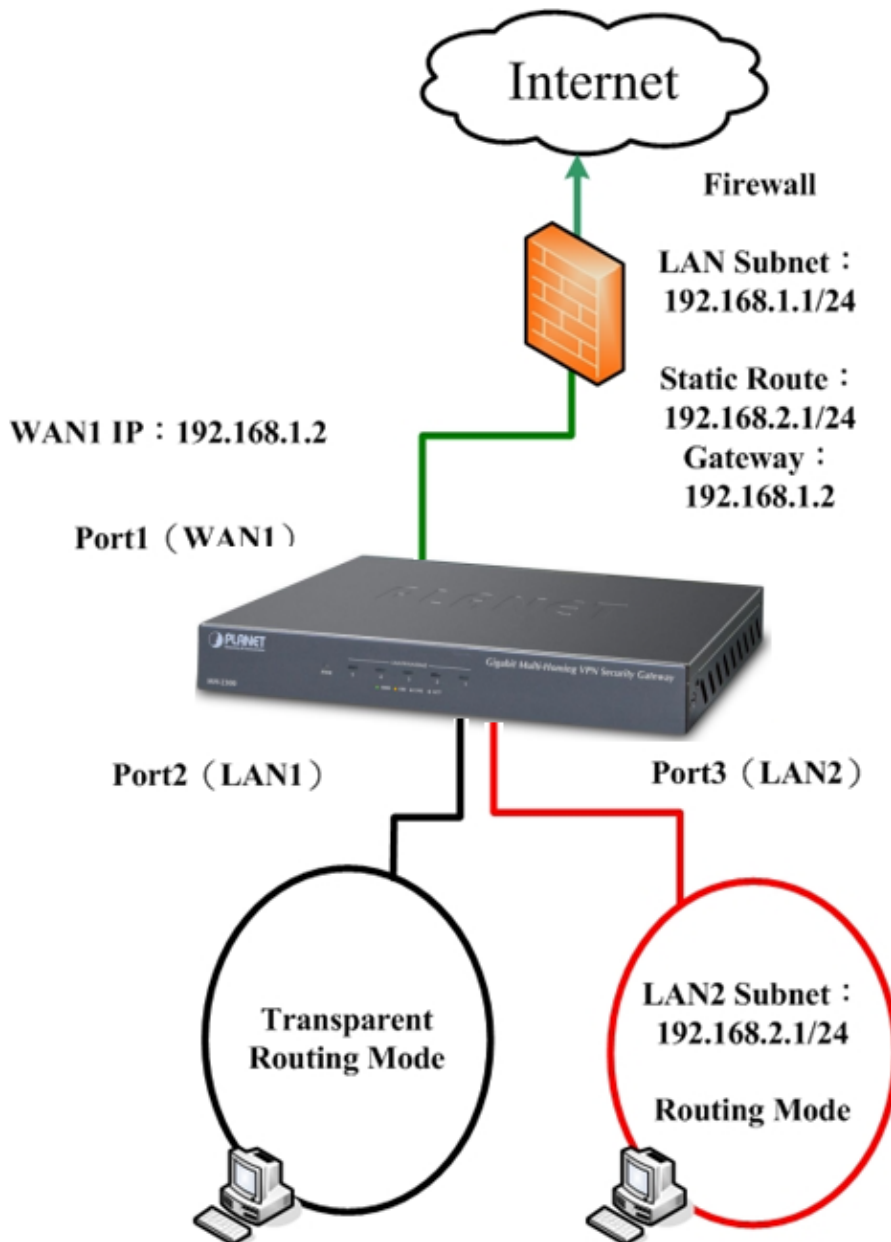
☒ Enable Any IP Routing Help

Access by / via : Help ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

OK
Cancel

Configuring the LAN Interface Settings

Step 3. The LAN subnets of 192.168.1.x/24 and 192.168.2.x/24 are now interconnected and are connected to the Internet through MH-2300.



The Deployment of LAN Subnets Routed through Transparent and NAT Mode

3.1.1.5 Deploying MH-2300 between a Gateway and Two Subnets (of which LAN Runs in NAT Routing Mode and DMZ Runs in Transparent Bridging Mode) to Manage the Internet Access of Internal Users

Prerequisite Configuration (Note: IP addresses are used as examples only)

On the existing firewall, specify a LAN subnet 172.16.x.x/16 (with the gateway set to 172.16.1.1)

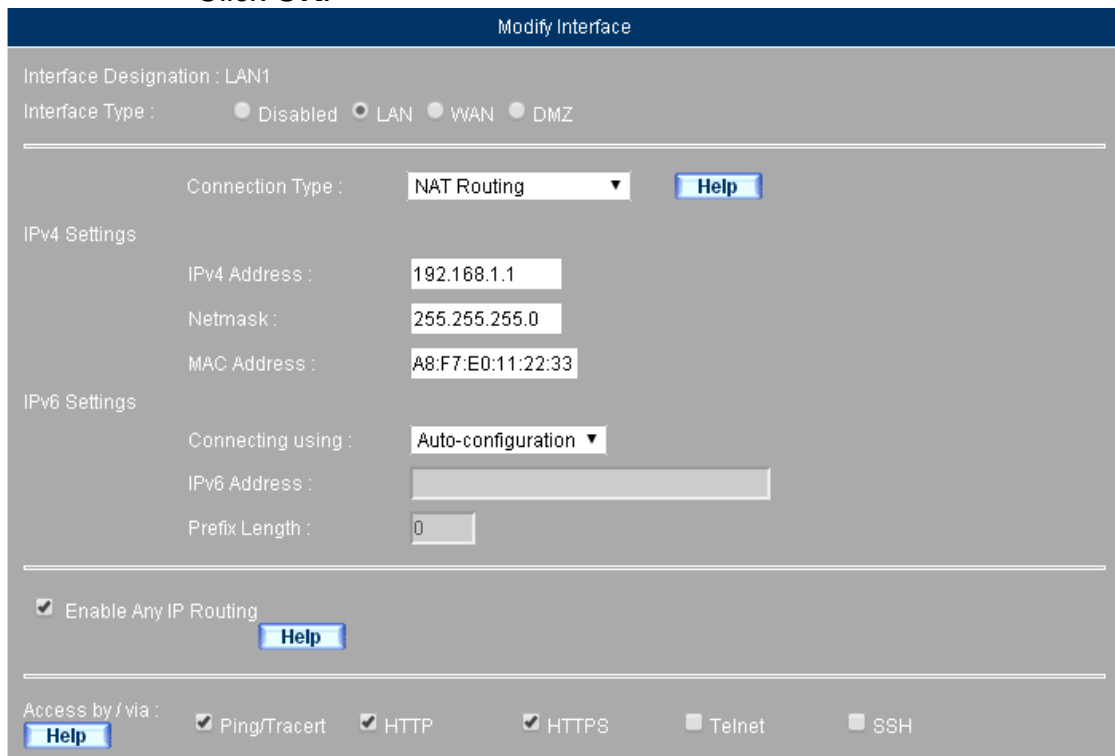
Configure Port1 as LAN1(192.168.1.1 in NAT Routing mode) to connect it to the LAN subnet 192.168.1.x/24, which is translated to 172.16.1.12 (WAN 1) for providing LAN users with Internet access.

Configure Port2 as WAN1(172.16.1.12) to connect it to the gateway (172.16.1.1).

Configure Port3 as DMZ1(in Transparent Bridging mode) to connect it to the LAN subnet 172.16.x.x/16 (with the gateway set to 172.16.1.1) for providing DMZ users with Internet access.

Step 1. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 1.
- Select "LAN" for **Interface Type**.
- Select "NAT Routing" for **Connection Type**.
- Specify the **IPv4 Address** and **Netmask**.
- Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- Click **OK**.



OK Cancel

Modifying the LAN Interface Settings

Step 2. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to Port 3.
- Select "DMZ" for **Interface Type**.
- Select "Transparent Bridging" for **Connection Type**.
- Tick the boxes of "Ping/ Tracer", "HTTP" and "HTTPS".
- Click **OK**.

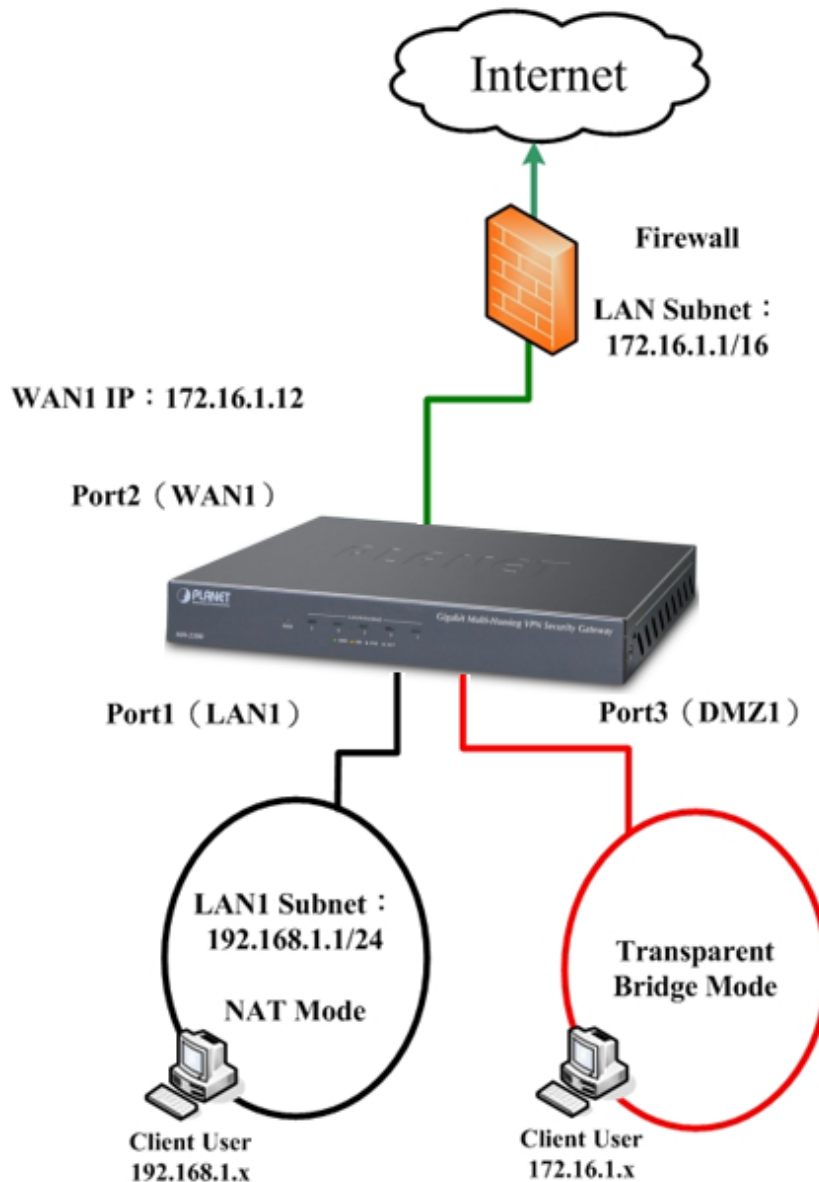
Modifying the DMZ Interface Settings

Step 3. Go to **Network > Interface Group** and then set as shown below:

- Select "Group 1" for **Port2(WAN1)** and **Port3(WAN2)**.
- Click **OK**.

Configuring the Interface Group Settings

Step 4. The DMZ subnet 172.16.x.x/16 is now connected to the Internet through MH-2300 via Transparent Bridging mode; also, the NAT-routed LAN subnet 172.16.1.12 is connected to the Internet using the public IP address.

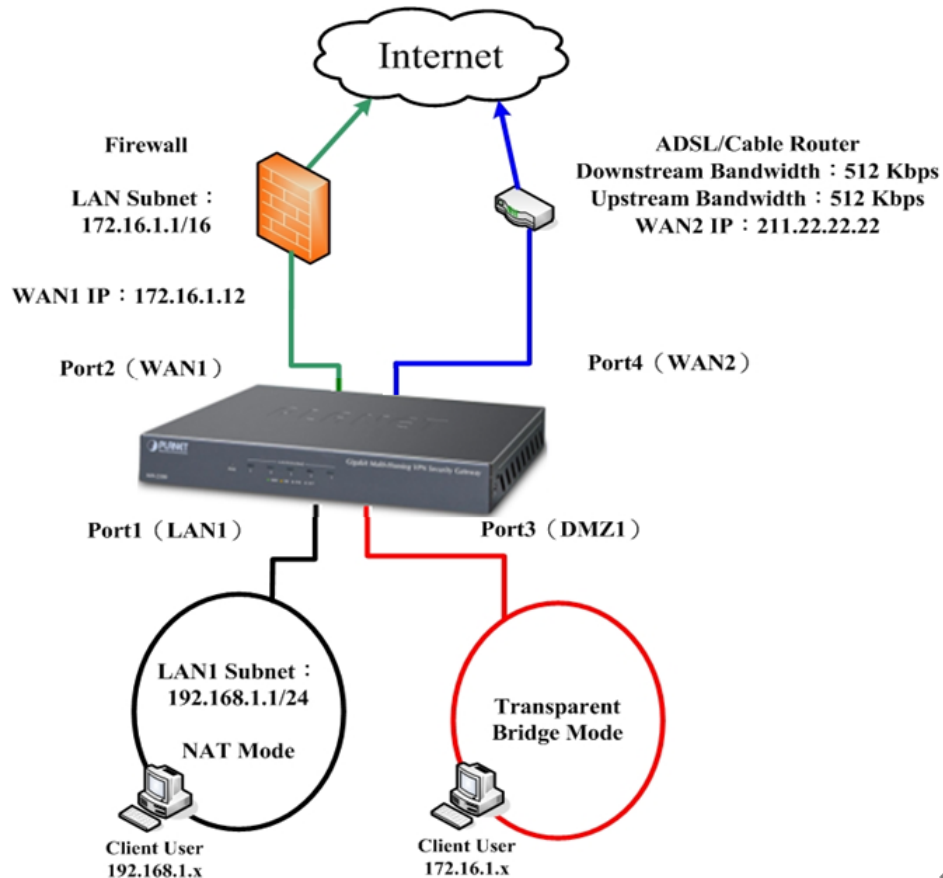


The 1st Deployment of a DMZ Subnet Routed through Transparent Bridging Mode

1. The DMZ subnet is connected to the Internet through the existing firewall.
2. If Port 4 is configured as WAN 2 (211.22.22.22) and is connected to the ADSL modem (ATUR) to access the Internet, then:
 - Specify DMZ subnet as 172.16.x.x/16
 - ◆ The PCs in the DMZ subnet with the gateway set to 172.16.1.1 are connected to the Internet using a public IP address via routing
 - ◆ The PCs in the DMZ subnet with the gateway set to 172.16.1.12 are connected to the Internet using the public IP addresses of WAN 1 (172.16.1.12 is NAT-routed) and WAN 2 (211.22.22.22) via load

balancing

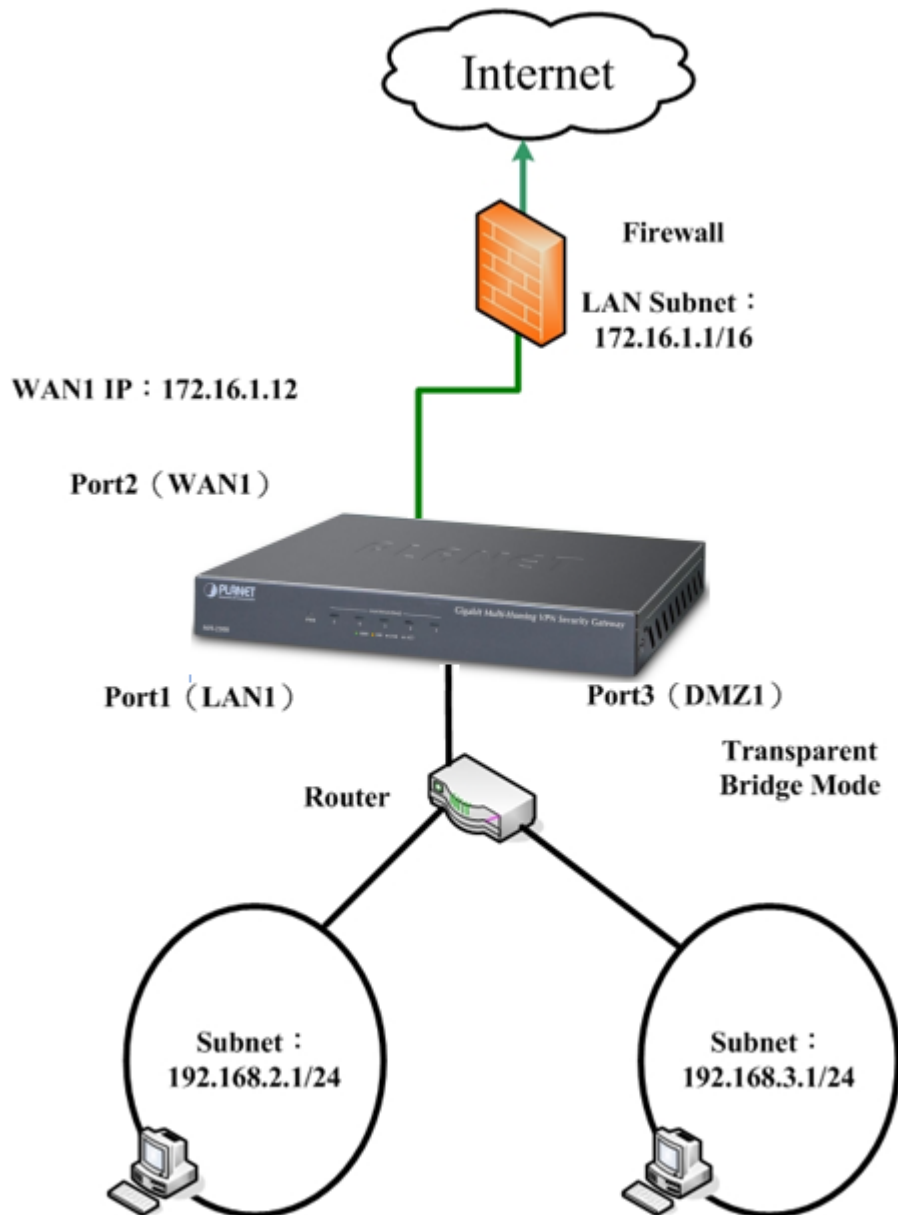
- Specify LAN subnet as 192.168.1.x/24:
 - ◆ The PCs in the LAN subnet with the gateway set to 192.168.1.1. are connected to the Internet using the public IP addresses of WAN 1 (172.16.1.12 is NAT-routed) and WAN 2 (211.22.22.22) via load balancing.



The 2nd Deployment of a DMZ Subnet Routed through Transparent Bridging Mode

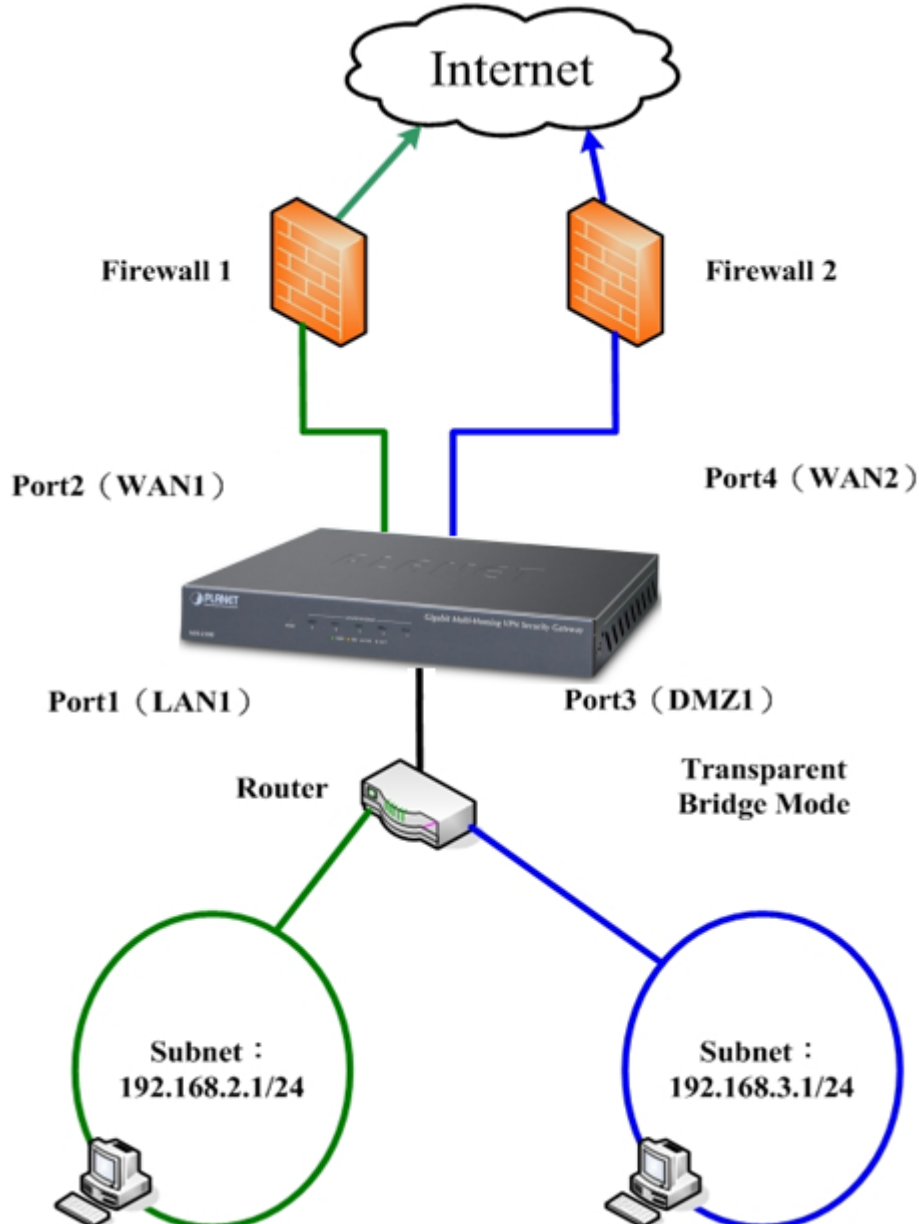
3. If a router and two WAN links are feasible, you may connect two LAN subnets and Port 3 (DMZ 1) to the router to provide internal users with Internet access, of which one subnet is routed to WAN 1 gateway and the other subnet is routed to WAN 2 gateway. The network packets will be processed according to the routing settings.

4. If a router is feasible, you may connect two LAN subnets to it to provide the Internet access using a public IP address via routing.



The 3rd Deployment of a DMZ Subnet Routed through Transparent Bridging Mode

5. If a router and two WAN links are feasible, you may connect two LAN subnets and Port 3 (DMZ 1) to the router to provide internal users with Internet access, of which one subnet is routed to WAN 1 gateway and the other subnet is routed to WAN 2 gateway. The network packets will be processed according to the routing settings.



The 4th Deployment of a DMZ Subnet Routed through Transparent Bridging Mode

3.1.1.6 Deploying MH-2300 between a Gateway and Two Subnets (of which LAN and DMZ Run in Transparent Bridge Mode) to Manage the Internet Access of Internal Users

Prerequisite Configuration (Note: The IP addresses are used as examples only)

On the existing firewall, specify a LAN subnet 192.168.1.x/24 (with the gateway

set to 192.168.1.1). Next, connect WAN port (61.11.11.11) to the ADSL modem (ATUR) to access the Internet and then run DMZ in Transparent mode.

Configure Port1 as WAN1 (192.168.1.2) and connect it to the gateway 192.168.1.1.

Configure Port2 as LAN1 (in Transparent Bridging mode) and connect it to the LAN subnet 192.168.1.x/24 (with the gateway set to 192.168.1.1) for providing LAN users with Internet access.

Configure Port3 as WAN2 (61.11.11.12) and connect it to the gateway (the DMZ subnet).

Configure Port4 as DMZ1 (Transparent Bridging mode) and connect it to the server in DMZ (using the public IP address of WAN 2). for providing Internet access via Transparent Bridging mode.

Step 1. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 1.
- Select “WAN” for **Interface Type**.
- Select your **Connection Type**.
- Configure the connection settings.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.

Modify Interface

Interface Designation : WAN1

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☒ Static IP Address (Leased Line User)
☐ Dynamic IP Address (Cable Modem User)
☐ PPPoE (ADSL Dial-Up User)

IPv4 Settings

IPv4 Address :
Netmask :
IPv4 Default Gateway :
MAC Address :

IPv6 Settings

Connecting using : ▼
IPv6 Address :
Prefix Length :
IPv6 Default Gateway :

Max. Downstream Bandwidth : Mbps (1 - 1000)
Max. Upstream Bandwidth : Mbps (1 - 1000)

Keepalive Properties :

[Help](#) Type : ▼
DNS IP Address :
Domain Name : (Max. 55 characters)
Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection : ▼

[Help](#)

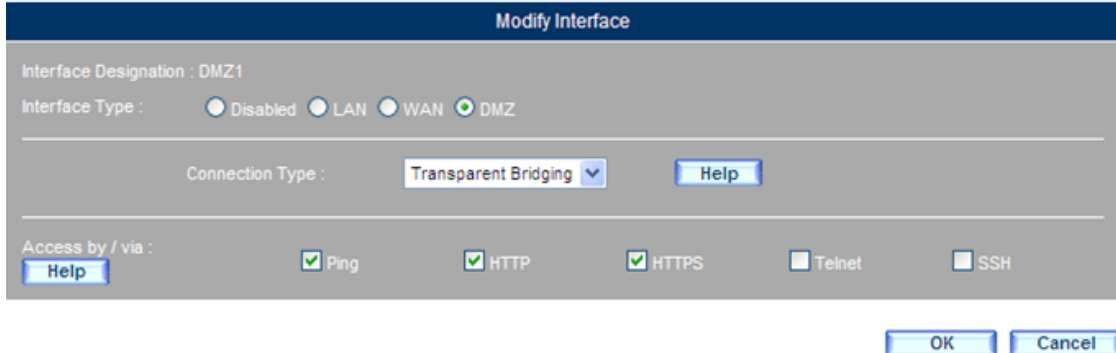
Access by / via : ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[Help](#)

Configuring the WAN Interface Settings

Step 2. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to Port 2.
- Select “LAN” for **Interface Type**.
- Select “Transparent Bridging” for **Connection Type**.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.



Interface Designation : DMZ1

Interface Type : ☐ Disabled ☐ LAN ☐ WAN ☒ DMZ

Connection Type : Transparent Bridging

Access by / via : ☒ Ping ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

Specifying the Connection Type for the LAN Interface

Step 3. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to Port 3.
- Select “WAN” for **Interface Type**.
- Select your **Connection Type**.
- Configure the connection settings.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.

Modify Interface

Interface Designation : WAN1

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☒ Static IP Address (Leased Line User)
☐ Dynamic IP Address (Cable Modem User)
☐ PPPoE (ADSL Dial-Up User)

IPv4 Settings

IPv4 Address :
Netmask :
IPv4 Default Gateway :
MAC Address :

IPv6 Settings

Connecting using : ▼
IPv6 Address :
Prefix Length :
IPv6 Default Gateway :

Max. Downstream Bandwidth : Mbps (1 - 1000)
Max. Upstream Bandwidth : Mbps (1 - 1000)

Keepalive Properties :

Type : ▼
DNS IP Address :
Domain Name : (Max. 55 characters)
Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection : ▼

Access by / via : ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

Configuring the WAN Interface Settings

Step 4. Under **Network > Interface**, set as shown below:

- Click **Modify** corresponding to Port 4.
- Select “DMZ” for **Interface Type**.
- Select “Transparent Bridging” for **Connection Type**.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.

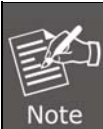
Specifying the Connection Type for the DMZ Interface

Step 5. Go to **Network > Interface Group** and then set as shown below:

Select “Group 1” for **Port1(WAN1)** and **Port2(LAN1)**.

- Select “Group 2” for **Port3(WAN2)** and **Port4(DMZ1)**.
- Click **OK**.
-

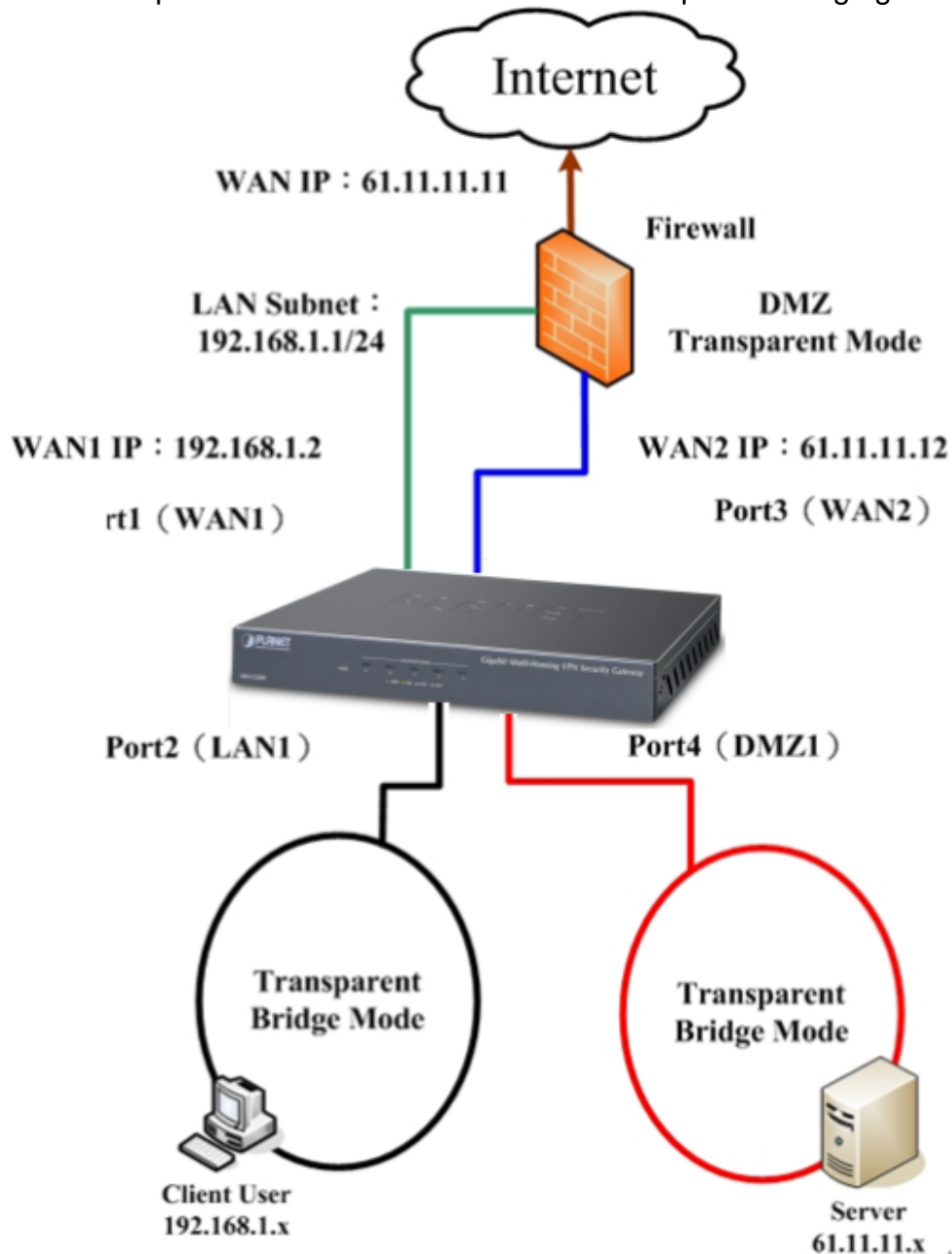
Configuring the Interface Group Settings



Note

After the completion of the above steps, the MH-2300 operates as two independent switches due to non-interconnected NIC groups, of which Group 1 (Port 1 and 2) provides Internet access to the LAN and Group 2 (Port 3 and 4) provides Internet access to the DMZ.

Step 6. The LAN subnet 192.168.1.x/24 is now connected to the Internet through MH-2300; also, the server in the DMZ subnet is accessible by the public IP address 61.11.11.12 in Transparent Bridging mode.



The Application of NIC Teaming

3.1.1.7 Using MH-2300 as a Gateway to Manage the Internet Access of Two LAN Subnets Separately via NAT Routing and Transparent Bridging Modes

Prerequisite Configuration (Note: IP addresses are used as examples only)

Configure Port1 as WAN1(61.11.11.11) and connect it to the ADSL modem (ATUR) to access the Internet.

Configure Port 2 as LAN1 (192.168.1.1 in NAT Routing mode) to connect it to the LAN subnet 192.168.1.x/24 (assumed it is connected to your sales department) to provide the Internet access using the public IP address 61.11.11.11.

Configure Port3 as LAN2 (192.168.1.1 in Transparent Bridging mode) to connect it to the LAN subnet 192.168.1.x/24 (assumed it is connected to your support department) to provide the Internet access using the public IP address 61.11.11.11.

The two LAN subnets are interconnected through network policies.

Step 1. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 1.
- Select "WAN" for **Interface Type**.
- Select your **Connection Type**.
- Configure the connection settings.
- Tick the boxes of "Ping/ Tracert", "HTTP" and "HTTPS".
- Click **OK**.

Modify Interface

Interface Designation : WAN1

Interface Type : ☐ Disabled ☐ LAN ☒ WAN ☐ DMZ

Connection Type : ☒ Static IP Address (Leased Line User)
☐ Dynamic IP Address (Cable Modem User)
☐ PPPoE (ADSL Dial-Up User)

IPv4 Settings

IPv4 Address :

Netmask :

IPv4 Default Gateway :

MAC Address :

IPv6 Settings

Connecting using :

IPv6 Address :

Prefix Length :

IPv6 Default Gateway :

Max. Downstream Bandwidth : Mbps (1 - 1000)

Max. Upstream Bandwidth : Mbps (1 - 1000)

Keepalive Properties :

[Help](#) Type :

DNS IP Address :

Domain Name : (Max. 55 characters)

Minimum Interval : second(s) (0 - 99, 0: no detection)

NAT Redirection :

[Help](#)

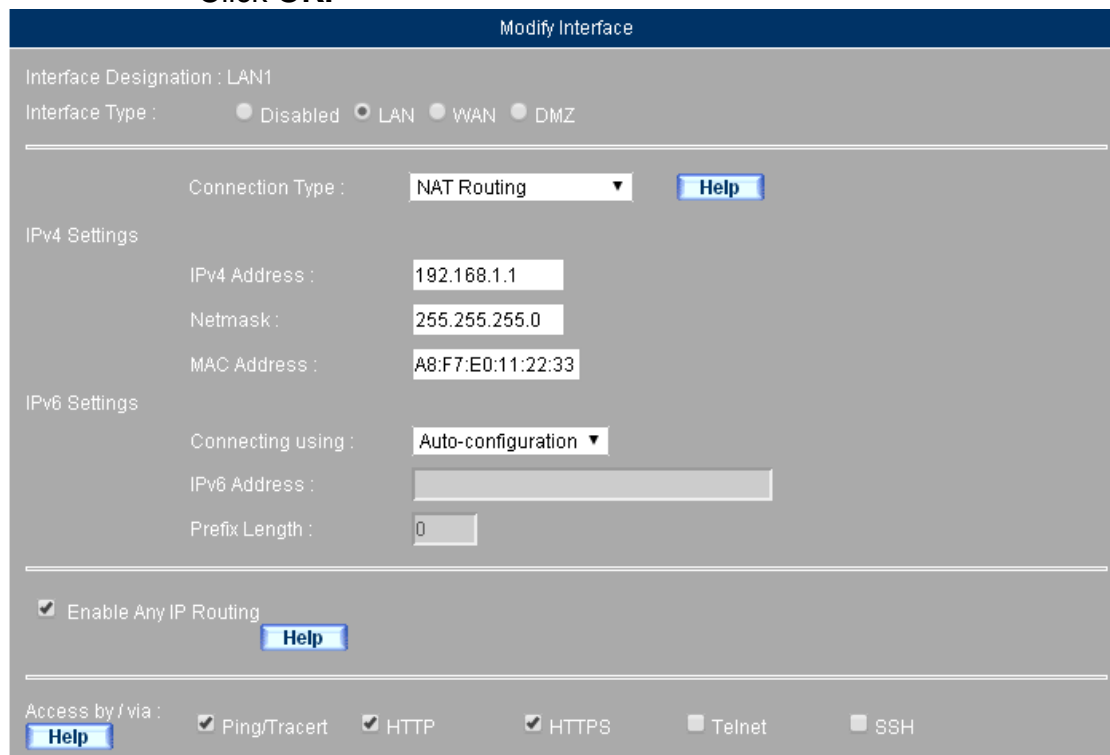
Access by / via : ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[Help](#)

Configuring the WAN Interface Settings

Step 2. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 2.
- Select “LAN” for **Interface Type**.
- Select “NAT Routing” for **Connection Type**.
- Specify the **IPv4 Address** and the **Netmask**.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.



Modify Interface

Interface Designation : LAN1

Interface Type : ☐ Disabled ☒ LAN ☐ WAN ☐ DMZ

Connection Type : NAT Routing [Help](#)

IPv4 Settings

IPv4 Address : 192.168.1.1

Netmask : 255.255.255.0

MAC Address : A8:F7:E0:11:22:33

IPv6 Settings

Connecting using : Auto-configuration

IPv6 Address :

Prefix Length : 0

☒ Enable Any IP Routing [Help](#)

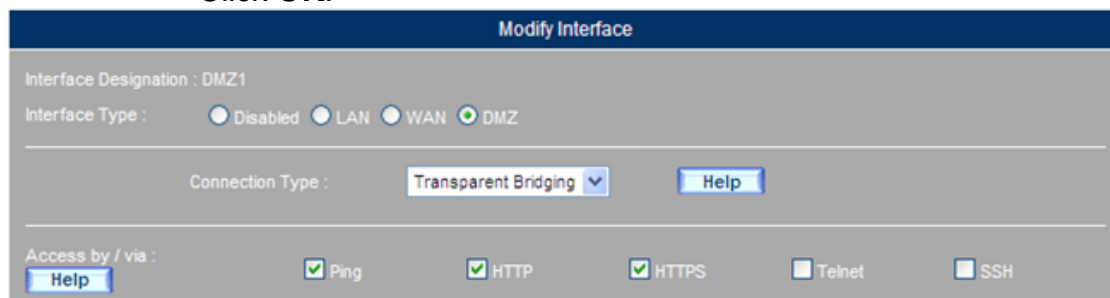
Access by / via : [Help](#) ☒ Ping/Tracert ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[OK](#) [Cancel](#)

Configuring the LAN Interface Settings

Step 3. Go to **Network > Interface** and then set as shown below:

- Click **Modify** corresponding to Port 3.
- Select “LAN” for **Interface Type**.
- Select “Transparent Bridging” for **Connection Type**.
- Tick the boxes of “Ping/ Tracert”, “HTTP” and “HTTPS”.
- Click **OK**.



Modify Interface

Interface Designation : DMZ1

Interface Type : ☐ Disabled ☐ LAN ☐ WAN ☒ DMZ

Connection Type : Transparent Bridging [Help](#)

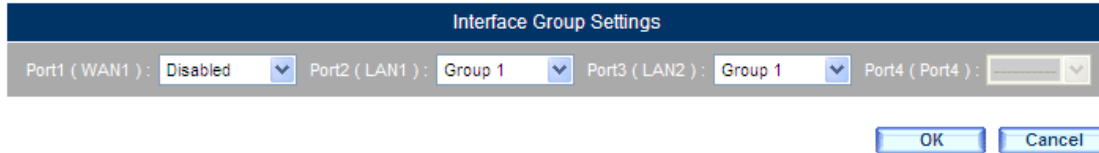
Access by / via : [Help](#) ☒ Ping ☒ HTTP ☒ HTTPS ☐ Telnet ☐ SSH

[OK](#) [Cancel](#)

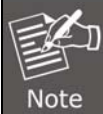
Specifying the Connection Type for the LAN Interface

Step 4. Go to **Network > Interface Group** and then set as shown below:
Select “Group 1” for **Port1 (WAN1)**, **Port2 (LAN1)** and **Port3 (LAN2)**.

- Click **OK**.

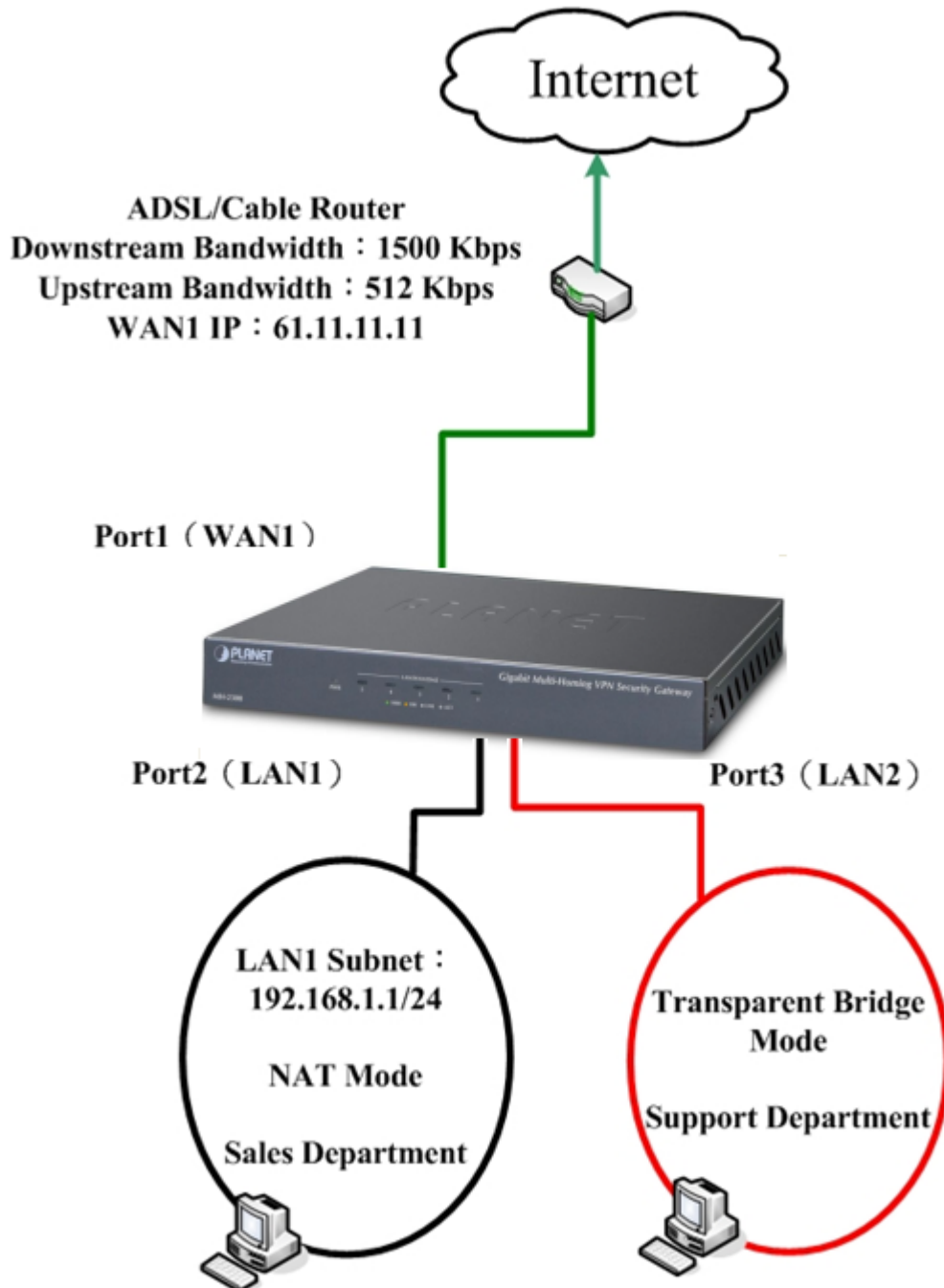


Configuring the Interface Group Settings



The LAN users from within the same subnet may be categorized by their department using the NIC ports. For example, sales department is connected to LAN 1 (Port 2) and customer support department is connected to LAN 2 (Port 3).

Step 5. The sales department from within LAN 1 and the customer support department from within LAN 2 are now interconnected through network policies and are connected to the Internet using the public IP address 61.11.11.11.



The Deployment of LAN Subnets Routed through Bridge and NAT Mode

Chapter 4. Policy Object

4.1 Address

This chapter will cover the configuration of *Address*, which allows for adding LAN, WAN and DMZ addresses and grouping addresses by purpose.

Each IP address can be assigned a friendly name and could represent a single host or a network subnet. IP addresses are categorized into three types, namely internal IP address, external IP address, and DMZ IP address. Group feature is available for address management to help simplify the process of applying addresses to network policies.



Once an address setting is created, it is ready for selection from the Source Address or Destination Address drop-down list in a network policy.

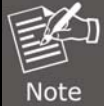
Terms in Address

Name

- Specify a friendly name for the address setting.

Address Type

- Specify the address by the netmask, prefix length, IP range or FQDN.



1. **FQDN** (Fully Qualified Domain Name) consists of Hostname and Domain Name. For example, "www.google.com.tw" is a FQDN; in this case, "www" is the hostname while "google.com.tw" is the domain name.
2. When it comes to website blocking, it takes more than just a website mapped IP (especially true for a website like Facebook and Yahoo), a network subnet, or a blacklist entry. **FQDN** provides a more effective means to block the access to a website by automatically parsing out all the mapped IP addresses.
3. **FQDN** is particularly designed to solve the shortness in blacklisting or whitelisting HTTPS and FTP addresses. It is available for configuration in WAN interfaces and can be applied to network policies.

IP Version

- The Internet protocol version for the address setting.

IP Address

- Specify the IP address of a host, or a network subnet, which can be an internal IP address, external IP address or DMZ IP address.

Netmask

- Enter 255.255.255.255 to match a single IPv4 address.
- Enter 255.255.255.0 to match a Class C IPv4 subnet, such as 192.168.100.x.

Prefix Length

- Enter 128 to match a single IPv6 address.
- Enter 64 to match an IPv6 subnet, such as 21DA:D3:0:2F3B.

MAC Address

- Bind the IP address to its MAC address to help manage the network access.

Interface

- Select the subnet that the IP address is located in.



Note

1. Under **Policy Object > Address > WAN Group**, the subnets from major ISPs in China including **China Unicom (CHU)**, **China Telecom (CHINA_TELECOM)**, **China Education (CHINA_EDU)** and **China Mobile (CHINA_MOBILE)** are added to support policy-based routing capability for the packets that are destined to any of these ISP networks.

● **This feature applies to a specific area only.**

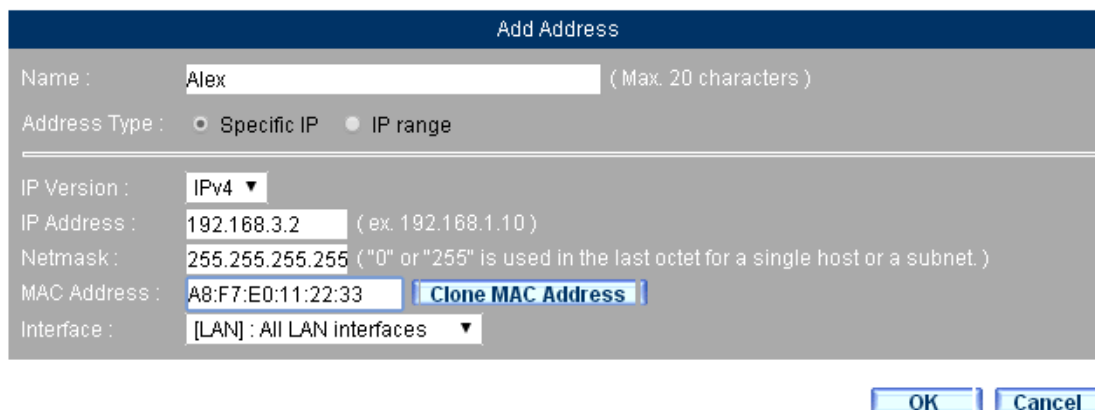
2. The address settings under **Policy Object > Address > LAN / DMZ** can be facilitated by clicking the **Assist Me** to automatically obtain addresses from **Monitor > Status > ARP Table / Sessions Info**.

4.1.1 Examples of Policy Creating

4.1.1.1 Creating a Policy to Allow Specific LAN Users the Access to FTP Service

Step 1. Under **Policy Object > Address > LAN**, set as shown below:

- Click **New Entry**.
- **Specify** a name for the LAN IP address.
- **Address Type**: Select either "Specific IP" or "IP range".
- **IP Version**: Select "IPv4" or "IPv6".
- **IP Address**: Specify the IP address of the user. (e.g., 192.168.3.2)
- **Netmask**: Enter "255.255.255.255" to match a single IPv4 address.
- **MAC Address**: Click **Clone MAC Address** to obtain the MAC address.
- Select the network subnet (interface) that the address resides in.
- Click **OK**.




Adding a LAN Address Entry



New Entry

LAN Address Successfully Added


Note

1. The network addresses created under **Policy Object > Address > WAN / LAN / DMZ** are available for export and import. You may export the addresses for editing and archival purposes and import them in the event of data loss.
2. For your easy configuration, the MAC address is also obtainable by clicking the **Clone MAC Address** button.
3. To manually bind an IP address to a MAC address, use **Assign Static IP** under **System > Configuration > DHCP**.
4. By default, each type of network has an address setting (i.e., the first

address entry) for covering the entire subnet, whether it is LAN, WAN, or DMZ.

5. The configuration of each type of network addresses are the same; yet, the configuration of **MAC address** and **Interface** are not available to WAN address settings.

Step 2. Go to **Policy > Outgoing** and then configure as below:

- **Source Address:** Select the previously created LAN address.
- **Service :** Select "FTP".
- Click **OK**.

Add Policy

Source Address : Alex

Destination Address : Outside Any

Service : FTP

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☒ Permit All ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (WAN1) ☐ Permit Port 2 (LAN1) ☐ Permit Port 3 (LAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

Creating a Policy to Allow the FTP Access to a LAN User

Source	Destination	Service	Action	Options	Configuration	Priority
Alex	Outside Any	FTP	✓		<div style="display: flex; justify-content: space-around; padding: 2px;"> Modify Remove Pause </div>	1

Policy Successfully Created

4.1.1.2 Creating a Policy to Allow a Users Group the HTTP Access

Step 1. Create the LAN addresses to be managed under **Policy Object > Address > LAN**.

Export data entries :

Import data entries : (Max. file size: 1 MB)

[Assist Me](#)

Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		<input type="button" value="In Use"/>
Alex	IPv4	All	192.168.1.2 / 255.255.255.255		<input type="button" value="Modify"/>
Jay	IPv4	All	192.168.1.4 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Tom	IPv4	All	172.19.100.79 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Miki	IPv4	All	192.168.85.85 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Eva	IPv4	All	172.19.100.101 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Creating LAN Addresses

Step 2. Under **Policy Object > Address > LAN Group**, set as shown below:

- Click **New Entry**.
- **Name:** Specify a friendly name for the address group.
- Select group members from the **Available address** column on the left, and then click **Add**.
- Click **OK**.

Add Address Group

Name : (Max. 20 characters)

===== [Available Addresses] =====

Miki

Eva

===== [Applied Addresses] =====

Alex

Tom

Jay

Grouping the LAN Addresses



Name	Group Members	Configuration
Test	Alex, Jay, Tom	<div> <div>Modify</div> <div>Remove</div> </div>



[New Entry](#)

Address Group Successfully Added



The configuration of each type of network address groups are the same.

Step 3. Go to **Policy Object > Address > WAN** and then configure as shown below:

- Click **New Entry**.
- **Name:** Specify a name for the address setting.
- **Address Type:** Select "Specific IP".
- **IP Version:** Select "IPv4".
- **IP Address :** Enter a public IP address.
- Click **OK**.

Add Address

Name : (Max. 20 characters)

Address Type : ☒ Specific IP ☐ IP range

IP Version :

IP Address : (ex. 192.168.1.10)

Netmask : ("0" or "255" is used in the last octet for a single host or a subnet.)

OK

Cancel

Adding a WAN Address

Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 1 MB)



Name	IP Version	IP Address / Netmask	Configuration
Outside Any	---	---	<div>In Use</div>
Yahoo	IPv4	202.1.237.21 / 255.255.255.255	<div>Modify</div> <div>Remove</div>



[New Entry](#)

WAN Address Successfully Added



How to resolve an IP address of a domain using FQDN feature:

- **Matching a domain keyword:** Type a domain keyword in the FQDN field to resolve the IP address of that domain name. For example, type "google" to match any domain contains google.
- **Matching a domain prefix:** Type the character "^" in the FQDN field to match the starting position within the domain. For example,

the expression “^mail.google” matches the domain beginning with “mail.google”.

- **Matching a domain postfix:** Type the character “\$” in the FQDN field to match the ending position within the domain. For example, the expression “google.com\$” matches the domain end with “google.com”.
- **Matching an exact domain:** Type the characters, “^” and “\$”, in the FQDN field to exactly match the domain, for example, the expression “^mail.google.com\$” only matches the domain “mail.google.com”.

Step 4. Under **Policy > Outgoing**, configure as shown below:

- **Source Address:** Select the previously created LAN address group.
- **Destination Address:** Select the previously created WAN address.
- Click **OK**.

Modify Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

☒ Permit All ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (WAN1) ☐ Permit Port 2 (LAN1) ☐ Permit Port 3 (LAN2) ☐ Permit Port 4 (Port4)


Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

Application Blocking :

 Advanced Settings

Creating a Policy to Allow the HTTP Access to a Group of LAN Users

1 / 1

Source	Destination	Service	Action	Options	Configuration	Priority
Test	Yahoo	Any	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

1 / 1

Policy Successfully Created

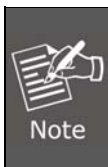


Address settings are required to apply to network policies to be practical and effective.

4.2 Service

Network services are provided through TCP and UDP protocols using different port numbers, such as Telnet port 23, FTP port 21, SMTP port 25, POP3 port 110, etc. MH-2300 provides TCP and UDP services by the two following categories:

- **Pre-defined:** The default TCP and UDP services, which are not removable.
- **Custom:** The user-definable TCP and UDP services, which allow the configuration of associated service ports.



Under **Policy Object > Service > Group**, group the desired services together and then apply it to a network policy so as to facilitate the management. For example, to allow a user (a specific IP address) to access five different services (HTTP, FTP, SMTP, POP3 and Telnet), it only takes a service group to achieve the management that originally requires five separate policies.

Terms in Service

Pre-defined

Symbol	Description
ANY	Any service that uses TCP or UDP protocol.
ICMP	Services that use ICMP protocol, such as Ping and Traceroute.
TCP	Services that use TCP protocol: AFPOverTCP, AOL, BGP, FINGER, FTP, GOPHER, HTTP, HTTPS, InterLocator, IRC, L2TP, LDAP, MSN, NetMeeting, NNTP, POP3, PPTP, Real-Media, RLOGIN, SMTP, SSH, TCP-Any, TELNET, Traceroute, VDO-Live, WAIS, WINFRAME, X-Windows, etc.
UDP	Services that use UDP protocol: DNS, IKE, IMAP, NFS, NTP, PC-Anywhere, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-Any, UUCP, etc.

Terms in Custom

Name

- The name of a custom service.

Protocol Type

- The protocol used for device communication. TCP and UDP are the most commonly used protocols among others.

Client Port

- The client-end port for protocol communication. It is recommended to use the default value.

Server Port

- The server-end port for a custom network service.

4.2.1 Example of Custom Service

4.2.1.1 Creating a Policy to Permit VoIP Telephony between External and Internal Users via TCP 1720, 15328-15333 and UDP 15328-15333

Step 1. Under **Policy Object > Address > LAN / LAN Group**, configure the following settings.

Export data entries :

Import data entries : (Max. file size: 1 MB)

[Assist Me](#)

Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		<input type="button" value="In Use"/>
VoIP_01	IPv4	All	192.168.1.2 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_02	IPv4	All	192.168.1.3 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_03	IPv4	All	192.168.1.4 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
VoIP_04	IPv4	All	192.168.1.5 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The Address Settings for VoIP Communication

Name ▲	Group Members	Configuration
VoIP_Group	VoIP_01, VoIP_02, VoIP_03, VoIP_04	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Grouping the LAN Addresses

Step 2. Under **Policy Object > Service > Custom**, configure as follows:

- **Name:** Specify a name for the service.
- In row No. 1, select **TCP**, leave the **Client Port** unchanged, and enter 1720 – 1720 for **Server Port**.
- In row No. 2, select **TCP**, leave the **Client Port** unchanged, and enter 15328 – 15333 for the **Server Port**.
- In row No. 3, select **UDP**, leave the **Client Port** unchanged, and enter 15328 – 15333 for the **Server Port**.
- Click **OK**.

Add User-Defined Service Help

Name : (Max. 20 characters)

No	Protocol Type (0 - 255)	Client Port (0 - 65535)	Server Port (0 - 65535)
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input style="width: 40px;" type="text" value="6"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="65535"/>	<input style="width: 40px;" type="text" value="1720"/> - <input style="width: 40px;" type="text" value="1720"/>
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other <input style="width: 40px;" type="text" value="6"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="65535"/>	<input style="width: 40px;" type="text" value="15328"/> - <input style="width: 40px;" type="text" value="15333"/>
3	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> Other <input style="width: 40px;" type="text" value="17"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="65535"/>	<input style="width: 40px;" type="text" value="15328"/> - <input style="width: 40px;" type="text" value="15333"/>
4	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>
5	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>
6	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>
7	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>
8	<input type="radio"/> TCP <input type="radio"/> UDP <input checked="" type="radio"/> Other <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/> - <input style="width: 40px;" type="text" value="0"/>

OK
Cancel

Adding a Custom Service


1 / 1 Go

Name ▲	Protocol Type	Client Port	Server Port	Configuration
VoIP	TCP	0 - 65535	1720 - 1720	<div style="display: flex; justify-content: space-around;"> Modify Remove </div>

1 / 1 Go

New Entry

A Custom Service Successfully Added

- 

Note

1. For most cases, the client-end port falls between 0 and 65535. It is recommended to use the default value.
 2. The two fields of **Client Port** and **Server Port** can be used to specify a port range (e.g., 15328:15333) or a single port (e.g., 1720:1720).

Step 3. Create a custom service under **Policy Object > Service > Custom** and then create a corresponding policy under **Policy Object > Virtual Server > Port Mapping**.

Name ▲	Public IP Address	Service	Private IP Address #	Configuration
VoIP	61.11.11.3 Port1 (WAN1)	VoIP	192.168.1.2 192.168.1.3 192.168.1.4 192.168.1.5 (LAN)	Modify Remove

[New Entry](#)

Service Successfully Applied to the Virtual Server Settings for Providing VoIP Service

Step 4. Under **Policy > Incoming**, configure as follows:

- **Destination Address:** Select the virtual server from the previous step.
- **Service:** Select the pre-defined service.
- Click **OK**.

Add Policy	
Source Address :	Outside Any
Destination Address :	[Port Mapping] VoIP(61.11.11.3)
Service :	VoIP
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	----- None -----
<input checked="" type="checkbox"/> Permit connections from Incoming <input type="checkbox"/> Deny connections from Incoming	
Reporting Mechanisms : Packet Logging : <input type="checkbox"/> Enabled Traffic Grapher : <input type="checkbox"/> Enabled	
<input type="checkbox"/> Advanced Settings	

[OK](#)

[Cancel](#)

Creating a Policy for Allowing Incoming VoIP Traffic

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](61.11.11.3)	VoIP	✓		Modify Remove Pause	1

[New Entry](#)

Policy Successfully Created

Step 5. Go to **Policy > Outgoing** and then configure as follows:

- **Source Address:** Select the LAN group.
- **Service:** Select the custom service.
- **Action:** Select "Port2 (WAN1)".
- Click **OK**.

Add Policy

Source Address : VoIP_Group ▼
Destination Address : Outside Any ▼
Service : VoIP ▼
Schedule : ----- None ----- ▼
Authentication : ----- None ----- ▼
VPN Trunk : ----- None ----- ▼

☐ Permit All
☐ Deny All

Action : Permit the selected:

☒ Permit Port 1 (WAN1)
☐ Permit Port 2 (LAN1)
☐ Permit Port 3 (WAN2)
☐ Permit Port 4 (Port4)

Reporting Mechanisms :
Packet Logging : ☐ Enabled
Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼
Application Blocking : ----- None ----- ▼

+ Advanced Settings

OK

Cancel

Creating a Policy for Allowing Outgoing VoIP Traffic


1 / 1

Source	Destination	Service	Action	Options	Configuration	Priority
VoIP_Group	Outside Any	VoIP	1		<div style="display: flex; justify-content: space-around; padding: 2px;"> Modify Remove Pause </div>	1 ▼

1 / 1

New Entry

Policy Successfully Created



Note

Service settings are required to apply to network policies to be practical and effective.

4.2.2 Example of Service Group

4.2.2.1 Grouping the Services and Creating a Policy to Permit Users to Access Network Services (HTTP, POP3, SMTP and DNS)

Step 1. Go to **Policy Object > Service > Group**, and then set as shown below:

- **Group Name:** Specify a name for the service group.
- Select HTTP, POP3, SMTP and DNS from the **Available Services** column on the left, and then click **Add**.
- Click **OK**.

Grouping the Services

Group Name	Group Items	Configuration
Main_Service	DNS, HTTP, POP3, SMTP	Modify Remove

New Entry

Service Group Successfully Added

Step 2. Go to **Policy Object > Address > LAN Group** and then create a LAN address group that is permitted to the network services.

Name	Group Members	Configuration
Sales	Alex, Eva, Tom	Modify Remove

New Entry

Address Group Successfully Added

Step 3. Under **Policy > Outgoing**, set as shown below:

- **Source Address:** Select the LAN address group from the previous step.
- **Service:** Select the service group.
- Click **OK**.

Add Policy

Source Address : Sales

Destination Address : Outside Any

Service : Main_Service

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☒ Permit All ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (WAN1) ☐ Permit Port 2 (LAN1) ☐ Permit Port 3 (WAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

+ Advanced Settings

Creating a Policy to Apply the Service Group Settings

1 / 1 Go

Source	Destination	Service	Action	Options	Configuration	Priority
Sales	Outside Any	Main_Servi...	✓		Modify Remove Pause	1

1 / 1 Go

Policy Successfully Created

4.3 Schedule

This chapter will cover the configuration of *Schedule*, which allows for assigning a time slot to each network policy. It helps you to achieve the most efficient network management.

Terms in Schedule

Name

- Specify a name for the schedule setting.

Type

- Two scheduling methods are available as follows:
 - ◆ **Recurring:** Policies are executed on the times specified on a weekly basis.
 - ◆ **One-Time:** Provides a start and stop time for a single specific duration based upon the year, month, day, hour and minute.

4.3.1 Examples of Schedule

4.3.1.1 Assigning Daily Internet Access Time Slots for LAN Users

Step 1. Under **Policy Object > Schedule > Settings**, set as shown below:

- Type the name.
- **Mode:** Select either **Recurring** or **One-Time**.
- Use the drop-down menus to select the required start and end time for each day of the week.
- Click OK.

Add Schedule

Name : (Max. 20 characters)

Type : ☒ Recurring ☐ One-Time

Day of the Week	Scheduled Time	
	Start At	End At
Sunday	Disabled	Disabled
Monday	08:30	18:30
Tuesday	08:30	18:30
Wednesday	08:30	18:30
Thursday	08:30	18:30
Friday	All Day	All Day
Saturday	Disabled	Disabled

Adding the Schedule Rule

/

Name ▲	Type	Time	Configuration
trading time	Recurring	Sunday	Disabled
		Monday	08 : 30 ~ 18 : 30
		Tuesday	08 : 30 ~ 18 : 30
		Wednesday	08 : 30 ~ 18 : 30
		Thursday	08 : 30 ~ 18 : 30
		Friday	All Day
		Saturday	Disabled
			<input type="button" value="Modify"/> <input type="button" value="Remove"/>

/

Step 2. Under **Policy > Outgoing**, set as shown below:

- Select the pre-defined schedule for **Schedule**.
- Click **OK**.

Add Policy

Source Address :

Inside Any

Destination Address :

Outside Any

Service :

Any

Schedule :

trading time

Authentication :

----- None -----

VPN Trunk :

----- None -----

☒ Permit All ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (WAN1)
 ☐ Permit Port 2 (LAN1)
 ☐ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging :

☐ Enabled

Traffic Grapher :

☐ Enabled

Web Filter :

----- None -----

Application Blocking :

----- None -----

[+ Advanced Settings](#)

Applying the Schedule to the Policy

1 / 1

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✔	🕒	<div style="display: flex; justify-content: space-around; font-size: small;"> Modify Remove Pause </div>	1

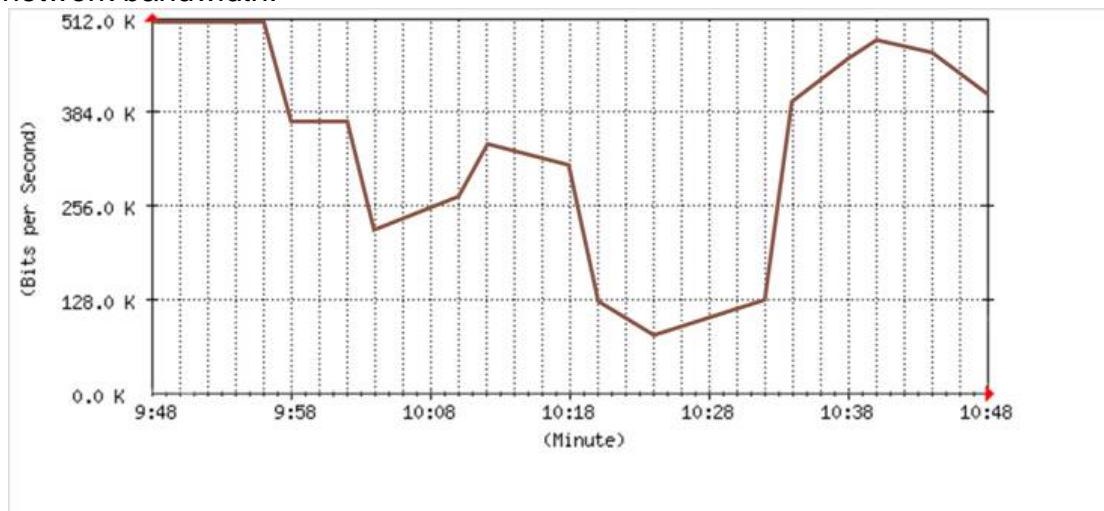
1 / 1

New Entry

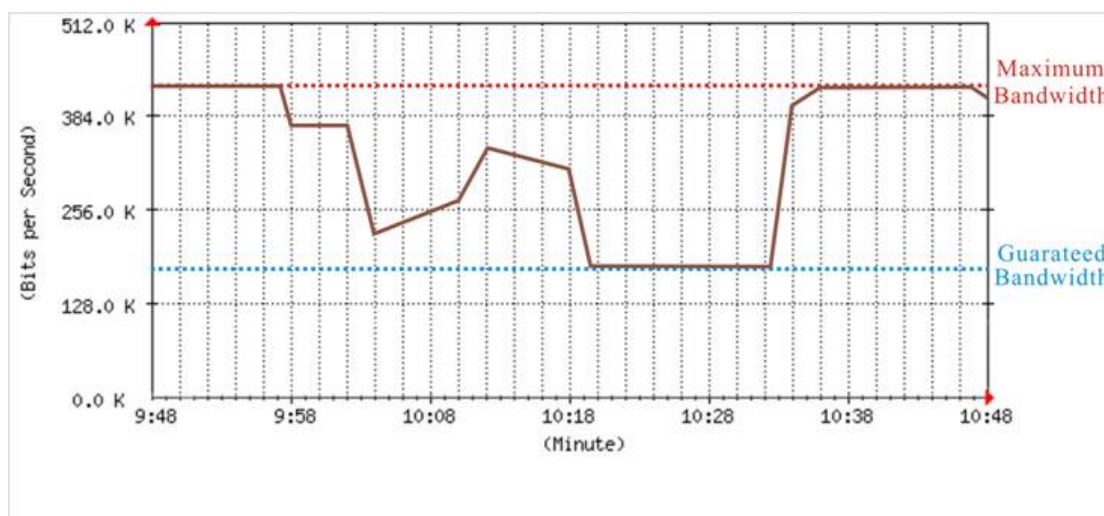
The Completed Policy Settings

4.4 QoS

This chapter will cover the configuration of QoS, which allows for applying QoS setting to a network policy to efficaciously allocate and manage the network bandwidth.



Before Applying QoS to the Network



After Applying QoS to the Network (Maximum: 400 Kbps, Guaranteed: 200 Kbps)

Terms in Settings

Name

- Specify a name for the QoS setting.

Interface

- The network interface that QoS is applied to.

Downstream Bandwidth

- Determine the guaranteed bandwidth and maximum bandwidth of the total downstream bandwidth.

Upstream Bandwidth

- Determine the guaranteed bandwidth and maximum bandwidth of the total upstream bandwidth.

Priority

- Prioritize the QoS settings to allocate the bandwidth.

G.Bandwidth

- Allocate the minimum (guaranteed) amount of bandwidth.

M.Bandwidth

- Allocate the maximum amount of bandwidth.

4.4.1 Example of Bandwidth Limitation

4.4.1.1 Creating a Policy to Limit Upload and Download Bandwidth

Step 1. Under **Policy Object > QoS > Settings**, set as shown below:

- Click **New Entry**. Type the **Name** accordingly.
- Configure the bandwidth of Port 2 (WAN1) and Port 3 (WAN2).
- Select the priority for this QoS setting.
- Click **OK**.


Add New Qos

Name : (Max. 20 characters)
Bandwidth Unit : Mbps ▼


Interface	Downstream Bandwidth		Upstream Bandwidth		Priority
1 (Disabled)	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	
2 (Disabled)	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	
3 (Disabled)	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	G.Bandwidth = <input type="text" value="0"/> Mbps	M.Bandwidth = <input type="text" value="0"/> Mbps	
4 (WAN2)	G.Bandwidth = <input type="text" value="200"/> Mbps (Range : 1 - 500)	M.Bandwidth = <input type="text" value="400"/> Mbps (Range : 1 - 500)	G.Bandwidth = <input type="text" value="200"/> Mbps (Range : 1 - 500)	M.Bandwidth = <input type="text" value="400"/> Mbps (Range : 1 - 500)	
5 (WAN1)	G.Bandwidth = <input type="text" value="300"/> Mbps (Range : 1 - 512)	M.Bandwidth = <input type="text" value="400"/> Mbps (Range : 1 - 512)	G.Bandwidth = <input type="text" value="50"/> Mbps (Range : 1 - 512)	M.Bandwidth = <input type="text" value="100"/> Mbps (Range : 1 - 512)	Medium ▼

OK
Cancel

Adding a QoS Rule



Name ▲	Interface	Downstream Bandwidth	Upstream Bandwidth	Priority	Configuration
	1 (LAN1)	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps		
	2 (LAN2)	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps		
Policy Qos	3 (Port3)	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps	G.Bandwidth = 0Mbps M.Bandwidth = 0Mbps	Medium	Modify Remove
	4 (WAN2)	G.Bandwidth = 200Mbps M.Bandwidth = 400Mbps	G.Bandwidth = 200Mbps M.Bandwidth = 400Mbps		
	5 (WAN1)	G.Bandwidth = 300Mbps M.Bandwidth = 400Mbps	G.Bandwidth = 50Mbps M.Bandwidth = 100Mbps		



[New Entry](#)

QoS Rule Successfully Added

Step 2. Under **Policy > Outgoing**, set as shown below:

- **QoS**: Select the QoS setting.
- Click **OK**.

Add Policy	
Source Address :	Inside Any ▼
Destination Address :	Outside Any ▼
Service :	Any ▼
Schedule :	----- None ----- ▼
Authentication :	----- None ----- ▼
VPN Trunk :	----- None ----- ▼
<input checked="" type="checkbox"/> Permit all outgoing connections <input type="checkbox"/> Deny all outgoing connections	
Action :	Permit the selected: <input type="checkbox"/> Port 1 (LAN1) <input type="checkbox"/> Port 2 (LAN2) <input type="checkbox"/> Port 3 (Port3) <input type="checkbox"/> Port 4 (WAN2) <input type="checkbox"/> Port 5 (WAN1)
Reporting Mechanisms : Packet Logging : <input type="checkbox"/> Enabled Traffic Grapher : <input type="checkbox"/> Enabled	
Web Filter :	----- None ----- ▼
Application Blocking :	----- None ----- ▼
<input type="checkbox"/> Advanced Settings	
QoS :	Policy Qos ▼
Max. Bandwidth Per Source IP :	Downstream <input type="text" value="0"/> Kbps / Upstream <input type="text" value="0"/> Kbps (0: unlimited)
P2P Bandwidth Limits :	Downstream <input type="text" value="0"/> Kbps / Upstream <input type="text" value="0"/> Kbps (0: unlimited)
Max. Concurrent Sessions Per IP :	<input type="text" value="0"/> (1 - 99999, 0: unlimited)
Max. Concurrent Sessions :	<input type="text" value="0"/> (1 - 99999, 0: unlimited)
Traffic Quota per Session :	<input type="text" value="0"/> KB (1 - 999999, 0: unlimited)

Traffic Quota Per Source IP : MB (1 - 999999, 0: unlimited)

Traffic Quota per Day : MB (1 - 999999, 0: unlimited)

IP Redirection :

Port 1 (LAN1) :

Port 2 (LAN2) :

Port 3 (Port3) :

Port 4 (WAN2) :

Port 5 (WAN1) :

[Help](#)


[OK](#) [Cancel](#)

Creating a Policy to Apply the QoS Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✓		Modify Remove Pause	1 ▼

[New Entry](#)

Policy Successfully Created



Please refer to the **Max. Upstream Bandwidth** and **Max. Downstream Bandwidth** in a WAN interface to create the corresponding QoS settings.

4.5 Authentication

This chapter will cover the configuration of *Authentication*, which allows for permitting the network access by verifying the identification via local authentication, group authentication, or other external authentication mechanisms, such as RADIUS, POP3 and LDAP.

Terms in Authentication

Authentication Settings

- The configuration is provided as follows:
 - ◆ **Authentication Port**: Specify a port number for authentication. By default, it is 82.
 - ◆ **Authentication Idle Timeout**: Specify a time to log out an idle user. By default, it is 30 minutes.

- ◆ **Log off users that have logged in for:** Specify a time for the validity of authentication. Once expired, users will be logged off.
- ◆ **Disable URL redirection for authentication:** To gain an access to the external network, the internal users should type <http://MH-2300 IP address:authentication port number> in the browser and then get authenticated on their own.
- ◆ **Allow password modification:** Once enabled, the local authentication accounts are allowed to modify their password.
- ◆ **Limit users to a single login session:** Once enabled, any subsequent login attempt to an authentication account is prohibited, despite whichever the authentication method is.
- ◆ **Identify source IP address by authentication name in the reportings:** Once enabled, the IP addresses of users monitored and managed by a system feature (e.g., Web Filter, Application Blocking, etc.) will be identified by their corresponding authentication name.
- ◆ **Disable case-sensitive matching for local authentication:** Once enabled, user authentication using a local account can be case insensitive.
- ◆ **Pre-Authentication Redirect URL:** Enter an URL address for users to be redirected to prior to the authentication. For this setting to be practical, the website or webpage that the URL linked to must be created on your own to embed the authentication scripts or to provide a hyperlink of <http://your web server's IP/your authentication website or webpage.html>, such as <http://210.59.123.456/authentication.html>.
- ◆ **Post-Authentication Redirect URL:** Enter an URL address for users to be redirected to after the authentication. You may leave the field blank (by default) to allow authenticated users direct access to their desired website.
- ◆ **Upload an image as the background for the authentication screen:** Allows for alternating the background of the authentication window.
- ◆ **Message for authentication users:** Compose the message (HTML supported) for the authentication screen. You may leave the field blank (by default) to use the system default message.
- ◆ **Message for successful authentications:** Compose the message (HTML supported) for a successful authentication. You may leave the field blank (by default) to use the system default message.
- ◆ **Message for failed authentications:** Compose the message (HTML supported) for a failed authentication. You may leave the field blank (by default) to use the system default message.
 - Go to **Policy Object > Authentication > Settings** and then configure as follows:

Authentication Settings
Help

Authentication Port : (1 - 65535, 0: disabled)

Authentication Idle Timeout : minute(s) (1 - 1000)

Log off users that have logged in for hour(s) (0 - 24, 0: unlimited)

☐ Allow password modification

☐ Limit users to a single login session

Post-Authentication Redirect URL : (Max. 80 characters)

Login Message: (Max. 4096 characters; HTML format supported) Preview

The Authentication Settings

- The authentication screen shown to a user who attempts to access the Internet.


User Login

Username :

Password :

Login

The Authentication Prompt Screen


 Note

1. The **Allow password modification** is only applicable to local authentication accounts under **Policy Object > Authentication > Account**.
2. The authentication screen is accessible directly at http://your_management_address:authentication_port_number, such as <http://192.168.139.1:82>.
3. Once the **Identify source IP address by authentication name in the reportings** is enabled, it will not be applied to the **Web Filter** reports (including operation logs and statistical reporting) until the next day.
4. For external user authentication, compose the authentication messages and configure as follows:
 - Enter the **Pre-Authentication Redirect URL** that is linked to a website or webpage which embeds the authentication scripts or provides a hyperlink of http://your_web_server_IP/your_authentication_website_or_webpage.html, such as

<http://210.59.123.456/authentication.html>.

- Compose the messages (HTML supported) separately for authentication users, successful authentications and failed authentications. (Note: Please copy the system default messages to a text file for backup before editing.)
- Users will be redirected to the pre-authentication website or webpage (click Preview for the authentication template next to **Message for authentication users** to build it) that contains the authentication scripts upon their Internet access.
 - ◆ The successful authentication message is shown when a valid set of credentials is supplied.
 - ◆ The failed authentication message is shown when an invalid set of credentials is supplied.

Authentication Settings		Help
Authentication Port :	<input type="text" value="82"/> (1 - 65535, 0: disabled)	
<input type="checkbox"/> Enable SSL encryption		
SSL Port :	<input type="text" value="0"/> (1 - 65535)	
Authentication Idle Timeout :	<input type="text" value="30"/> minute(s) (1 - 1000)	
Log off users that have logged in for	<input type="text" value="0"/> hour(s) (0 - 24, 0: unlimited)	
<input type="checkbox"/> Disable URL redirection for authentication		
<input type="checkbox"/> Allow password modification		
<input type="checkbox"/> Limit users to a single login session		
<input type="checkbox"/> Identify source IP address by authentication name in the reportings		
<input type="checkbox"/> Disable case-sensitive matching for local authentication		
Pre-Authentication Redirect URL :	<input type="text" value="61.11.11.12/auth.html"/> (Max. 80 characters)	
Post-Authentication Redirect URL :	<input type="text"/> (Max. 80 characters)	
Upload an image as the background for the authentication screen: <input type="button" value="Browse.."/>		
Preview		
(Max. file size:50 KB; Resolution : 1022 x 622 pixels; File types : jpg, jpeg, jpe, gif, bmp, png...)		

Message for authentication users: (Max. 1024 characters; HTML format supported) [Preview](#)

Message for successful authentications: (Max. 1024 characters; HTML format supported) [Preview](#)

```
<html>
<head>
<title>User Authentication</title>
<link rel="stylesheet" href="http://192.168.139.11:82/my_style.css"
type="text/css">
<meta http-equiv=Content-Type content="text/html; charset=UTF-8">
<meta http-equiv="pragma" content="no-cache">
<script type="text/javascript">
var id = null;
var width = 570;
```

Message for failed authentications: (Max. 1024 characters; HTML format supported) [Preview](#)

```
<html>
<head>
<title>User Authentication - Login</title>
<link rel="stylesheet" href="http://192.168.139.11:82/my_style.css"
type="text/css">
<meta http-equiv=Content-Type content="text/html; charset=UTF-8">
<meta http-equiv="pragma" content="no-cache">
<script type="text/javascript"
src="http://192.168.139.11:82/global.js"></script>
<script type="text/javascript"
```

Composing the Authentication Messages

"Authentication
Successful"

The Successful Authentication Message

User Login	
Username :	<input type="text" value="ines"/>
Password :	<input type="password" value="****"/>
<input type="button" value="Login"/>	

Supplying an Invalid Set of Credentials

Username not found or incorrect password !
<input type="button" value="OK"/>

Terms in Account

Account Name

- Specify a name for the local authentication.

Password

- Specify a password for the local authentication.

Confirm Password

- Repeat the password in this field.

Force password change at initial login

- Once enabled, users will be forced to change their password at the first login.

The account is valid through

- Specify a date for the authentication validity.

Terms in RADIUS

RADIUS Server Shared Secret

- Specify a password for the RADIUS authentication.

Enable 802.1x RADIUS server authentication

- Once enabled, the RADIUS authentication will perform IEEE 802.1x port-based network access control.

RADIUS Account

- List the RADIUS accounts which can be grouped for authentication.

Terms in LDAP

LDAP Base DN

- Specify a distinguished name for the LDAP server.

LDAP Bind DN

- Specify a user that is allowed a search within the LDAP directory.

Username

- Specify a name for the LDAP authentication.

LDAP User Name

- Group the LDAP users by their department to facilitate authentication.

4.5.1 Local / Group Authentication

4.5.1.1 Managing Internet Access with A Local Authentication Group

Step 1. Under **Policy Object > Authentication > Account**, add the users to be authenticated.

Export data entries :


Import data entries : (Max. file size: 20 KB)

/ 1

Account Name ▲	Expiry Date	Configuration
Ines		<input type="button" value="Modify"/>
Anthony		<input type="button" value="Modify"/>
Brandon		<input type="button" value="Modify"/>

/ 1

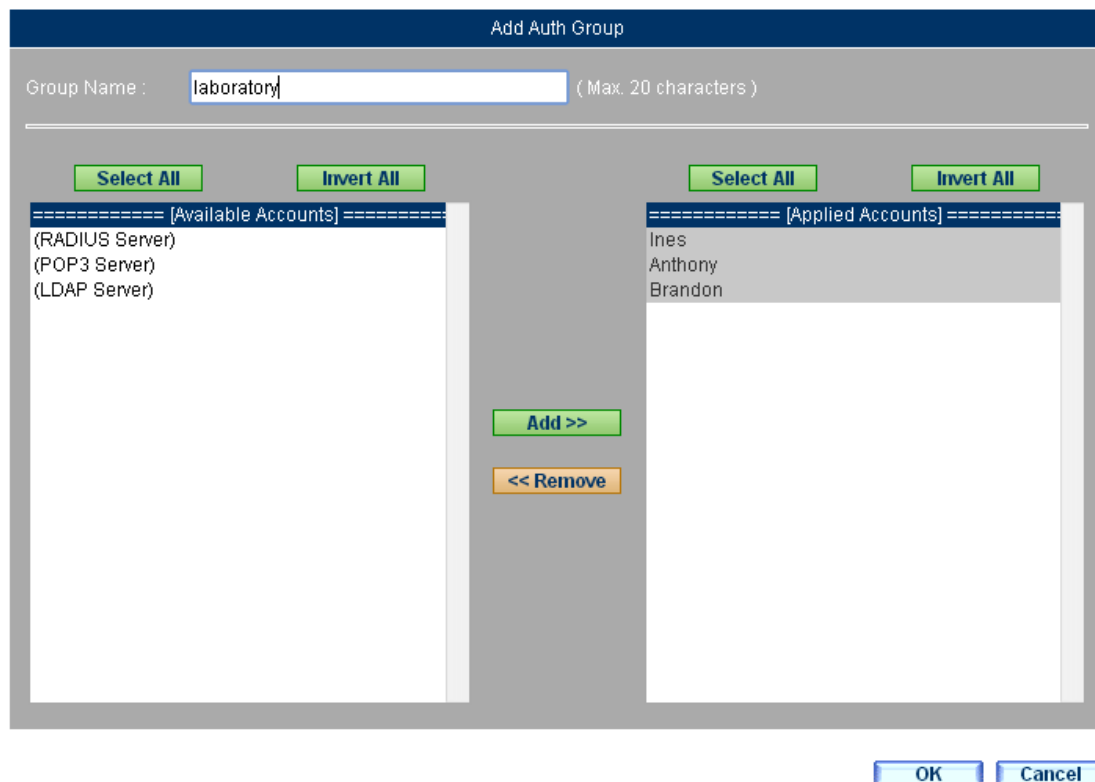
The User Accounts for Authentication


Note

1. The local authentication users are available for export and import. You may export the entries for editing and archival purposes and import them in the event of data loss.
2. Local authentication requires the **Preferred DNS server** on the local PCs to be specified as same as the LAN interface to be effective. For further information on configuring **Preferred DNS server**, please refer to:
<http://windows.microsoft.com/en-US/windows-vista/Change-TCP-IP-settings>

Step 2. Under **Policy Object > Authentication > Group**, set as shown below:

- Click **New Entry**.
- **Group Name**: Specify a name for the authentication group.
- Select group members from the **Available Accounts** column on the left, and then click **Add**.
- Click **OK** to complete the settings.



Add Auth Group

Group Name : (Max. 20 characters)

Select All **Invert All**

===== [Available Accounts] =====

(RADIUS Server)
(POP3 Server)
(LDAP Server)

Select All **Invert All**

===== [Applied Accounts] =====

Ines
Anthony
Brandon

Add >>
<< Remove

OK
Cancel

The Group Setting for User Authentication

Step 3. Go to **Policy > Outgoing** and then configure as follows:

- **Authentication:** Select the authentication group.
- Click **OK** to complete the settings.

Comment:

Add Policy

Source Address :	Inside Any ▼
Destination Address :	Outside Any ▼
Service :	Any ▼
Schedule :	----- None ----- ▼
Authentication :	laboratory ▼
VPN Trunk :	----- None ----- ▼

☒ Permit all outgoing connections
 ☐ Deny all outgoing connections

Action :

Permit the selected:

☐ Port 1 (LAN1)
 ☐ Port 2 (LAN2)
 ☐ Port 3 (Port3)
 ☐ Port 4 (WAN2)
 ☐ Port 5 (WAN1)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼

Application Blocking : ----- None ----- ▼

± Advanced Settings

Creating a Policy to Apply the Authentication Group Settings

1 / 1

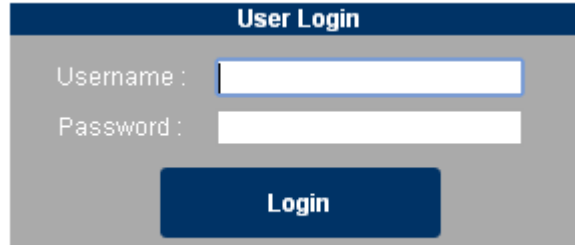
Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1 ▼

1 / 1

New Entry

Policy Successfully Created

Step 4. The group members will be prompted for their authentication credentials to access the Internet. Click **Login** to complete the authentication procedure.



The image shows a web form titled "User Login". It has a dark blue header bar with the title. Below the header, there are two input fields: "Username :" and "Password :". Each field has a white text box with a blue border. Below the password field is a dark blue button with the word "Login" in white text.

The Authentication Prompt Screen

Step 5. To log out of authentication session, click **Logout** **Authentication-User** in the pop-up window (appeared when being authenticated; if it has been closed, open it again by going to http://your_management_address:authentication_port_number/logout.html, such as <http://192.168.139.11:82/logout.html>)



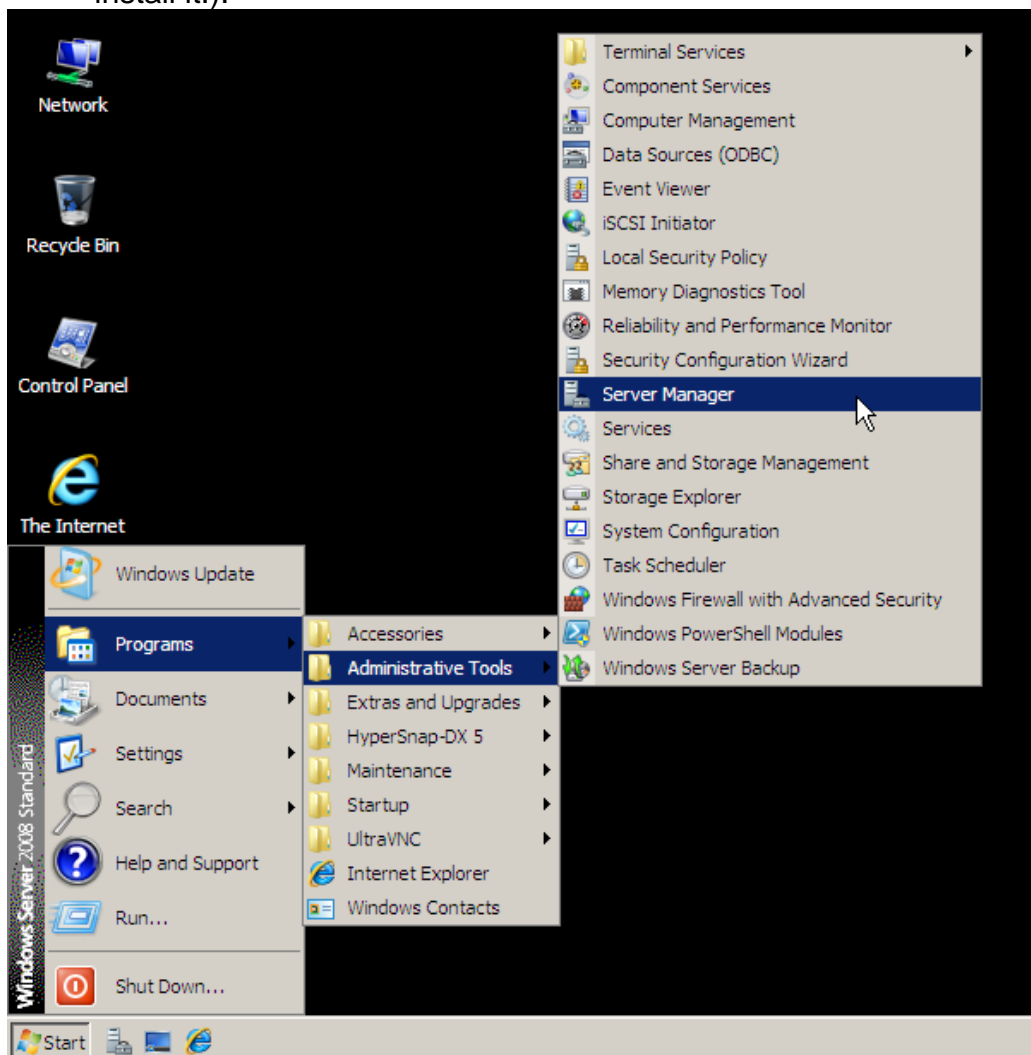
The Authentication Logout Window

4.5.2 RADIUS Authentication

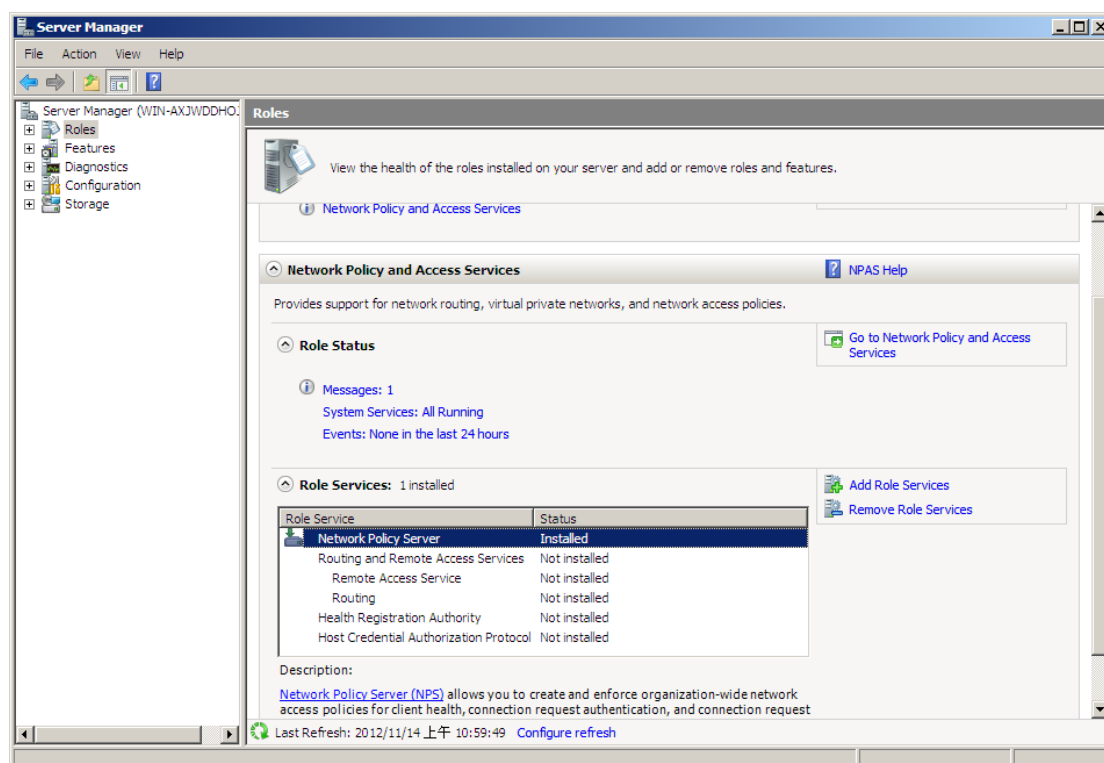
4.5.2.1 Managing Internet Access with a Windows 2008 RADIUS Server

※ **Setting up a Windows 2008 RADIUS Server**

Step 1. Go to **Start > Programs > Administrative Tools > Server Manager**. Next, in the **Server Manager** tree panel, expand **Roles** to check the availability of **Network Policy Server** (appeared as an installed role service on the right panel, if not installed, click [Add Role Services](#) to install it.).



Selecting the Server Manager on the Start Menu

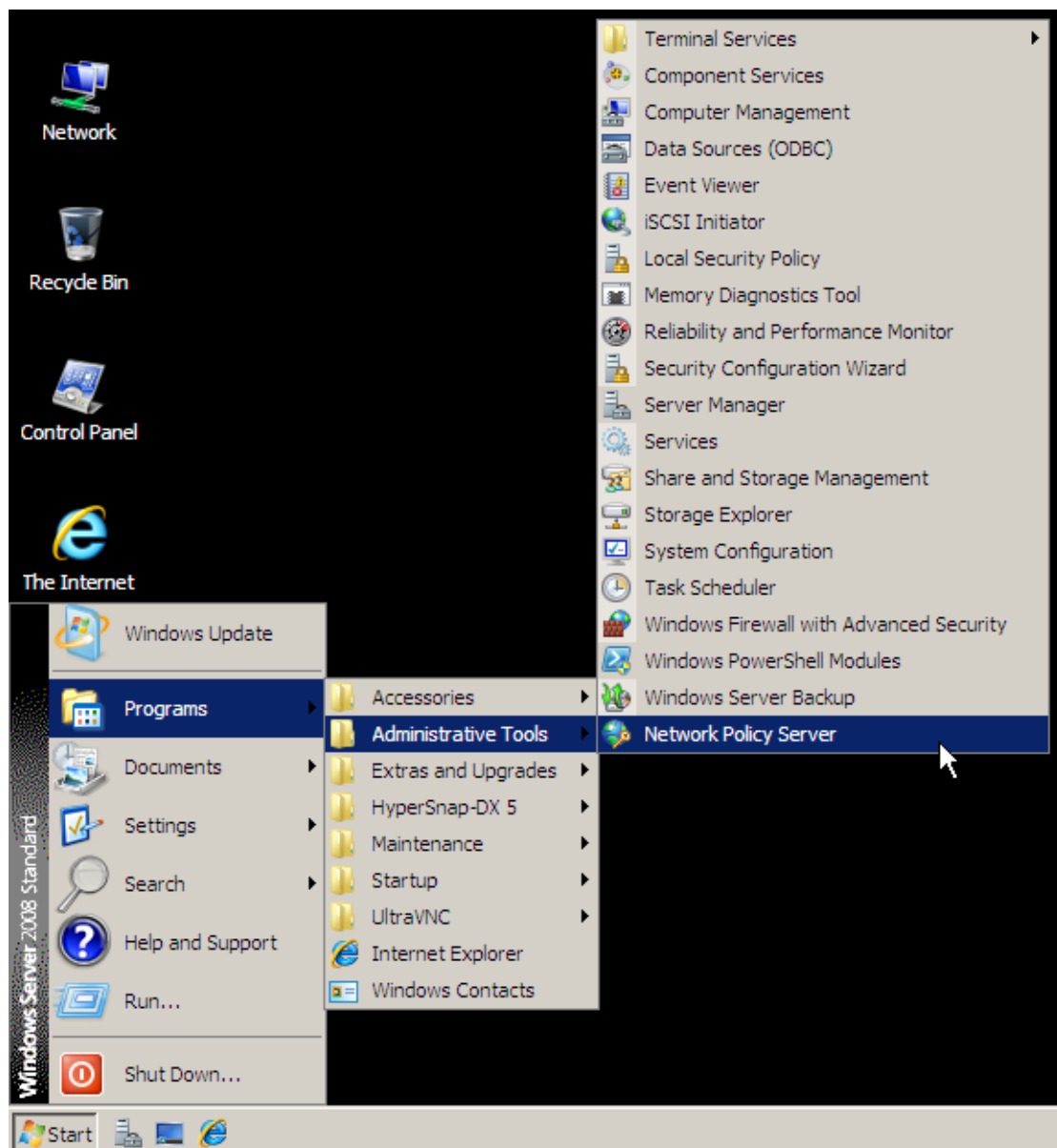


Checking the Availability of Network Policy Server

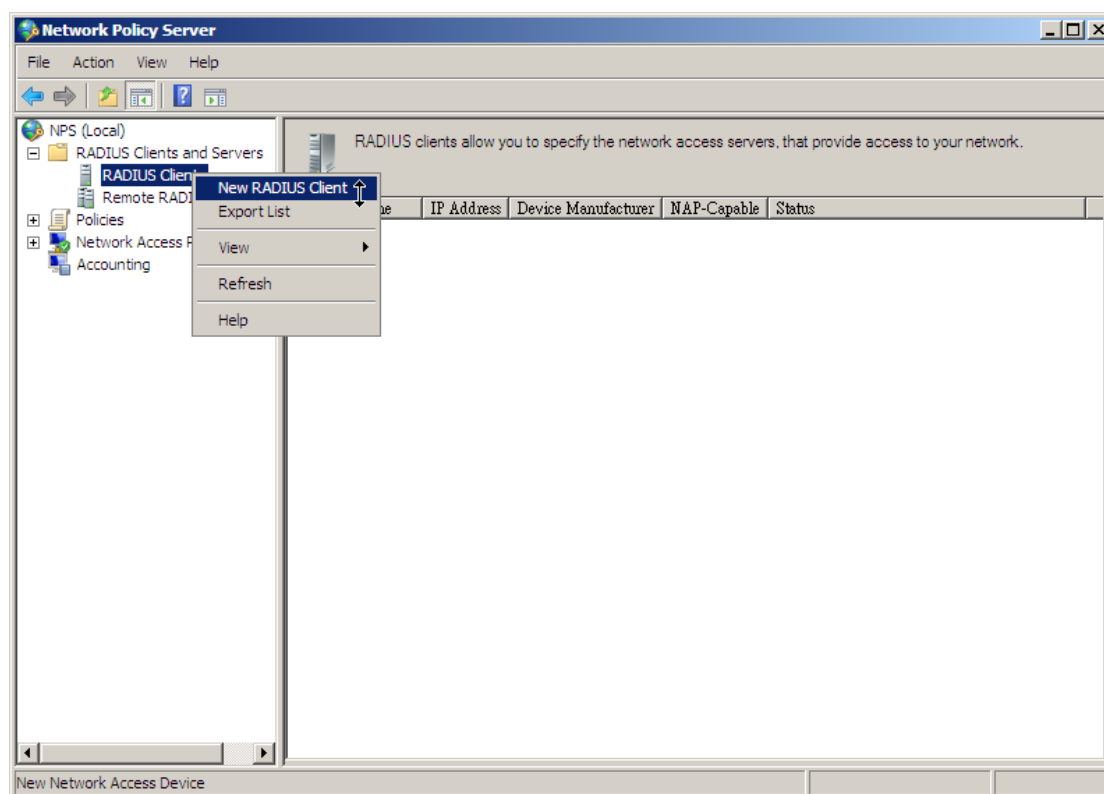
Step 2. Go to **Start > Programs > Administrative Tools > Network Policy Server** and then set as shown below:

- In the **NPS (Local)** tree panel, expand **RADIUS Clients and Servers**, right-click **RADIUS Client**, and then select **New RADIUS Client**.
- In the **New RADIUS Client** dialog box, set as shown below:
 - ◆ Tick the box of **“Enable this RADIUS client”**.
 - ◆ Specify a friendly name for the RADIUS client.
 - ◆ Type in the management address in the **Address (IP or DNS)** field.
 - ◆ **Vendor name:** Select **“RADIUS Standard”**.
 - ◆ **Shared Secret:** Select the radio box of **“Manual”** and specify the corresponding **Shared secret**.
 - ◆ Click **OK** to complete the settings.
- In the **NPS (Local)** tree panel, expand **Policies**, right-click **Network Policies**, and then select **New**.
- In the **New Network Policy** dialog box, set as shown below:
 - ◆ Specify a name for the network policy.
 - ◆ Select the radio box of **“Type of network access server”** and select **“Unspecified”** from the corresponding drop-down list.
 - ◆ Click **Next**.
 - ◆ Click **Add**.
 - ◆ In the **Select condition** dialog box, select **“Service Type”** and then click **Add**.
 - In the **Service Type** dialog box, tick the boxes of **“Framed”** and **“Authentication Only”** and then click **OK**.

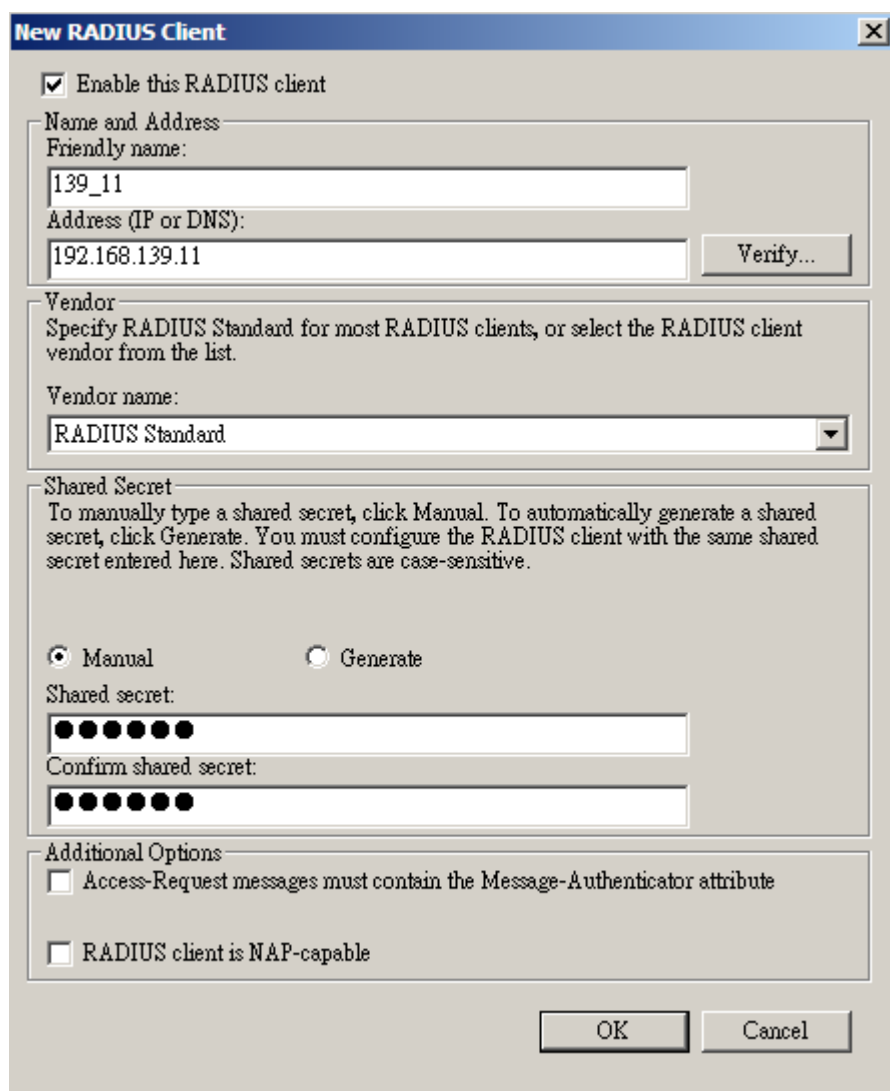
- ◆ Click
- ◆ Tick the box of “Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)”, “Microsoft Encrypted Authentication (MS-CHAP)”, “Encrypted authentication (CHAP)”, and “Unencrypted authentication (PAP, SPAP)”.
- ◆ Click **Next**.
- ◆ Click **Next**.
- ◆ Click **Edit** to change the attribute values of **Framed-Protocol** and **Service-Type**. For **Framed-Protocol**, select the radio box of “Commonly used for Dial-Up or VPN” and select “PPP” from the corresponding drop-down list; for **Service-Type**, select the radio box of “Commonly used for Dial-Up or VPN” and select “Framed” from the corresponding drop-down list.
- ◆ Click **Next**.
- ◆ Click **Finish** to complete the settings.



Selecting the Network Policy Server on the Start Menu



Selecting the New RADIUS Client from the Shortcut Menu



New RADIUS Client

☒ Enable this RADIUS client

Name and Address

Friendly name:
139_11

Address (IP or DNS):
192.168.139.11 Verify...

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:
●●●●●●

Confirm shared secret:
●●●●●●

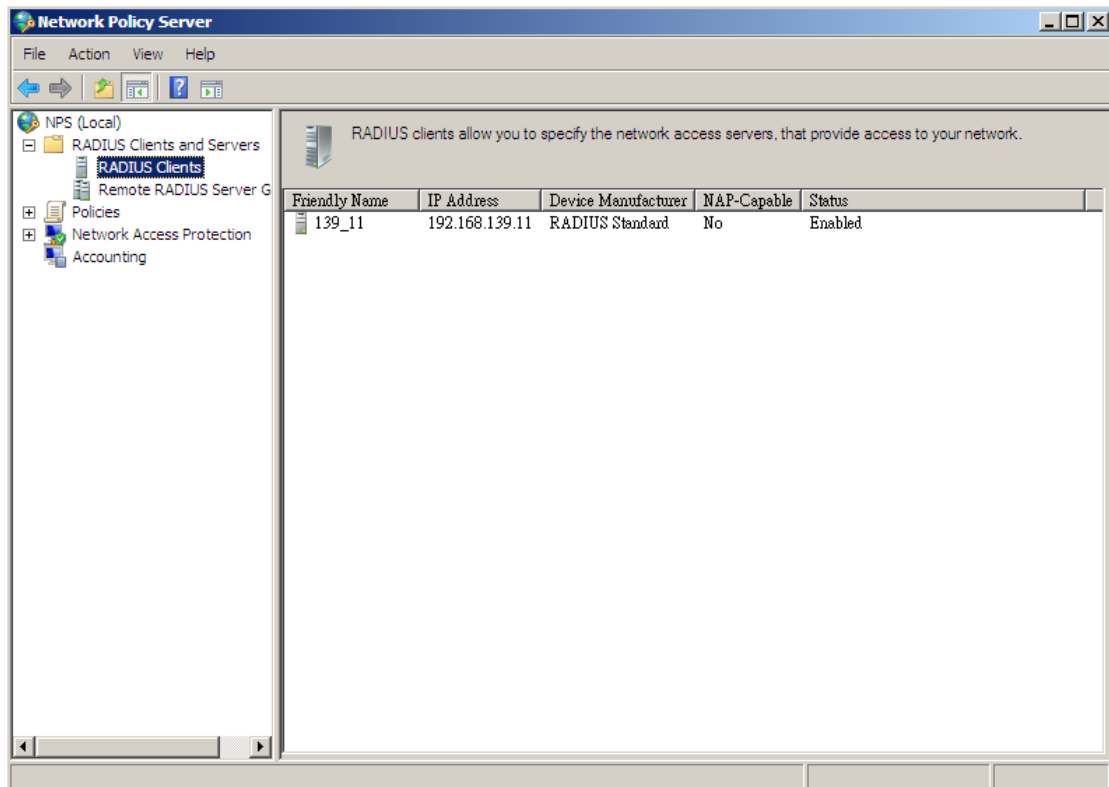
Additional Options

☐ Access-Request messages must contain the Message-Authenticator attribute

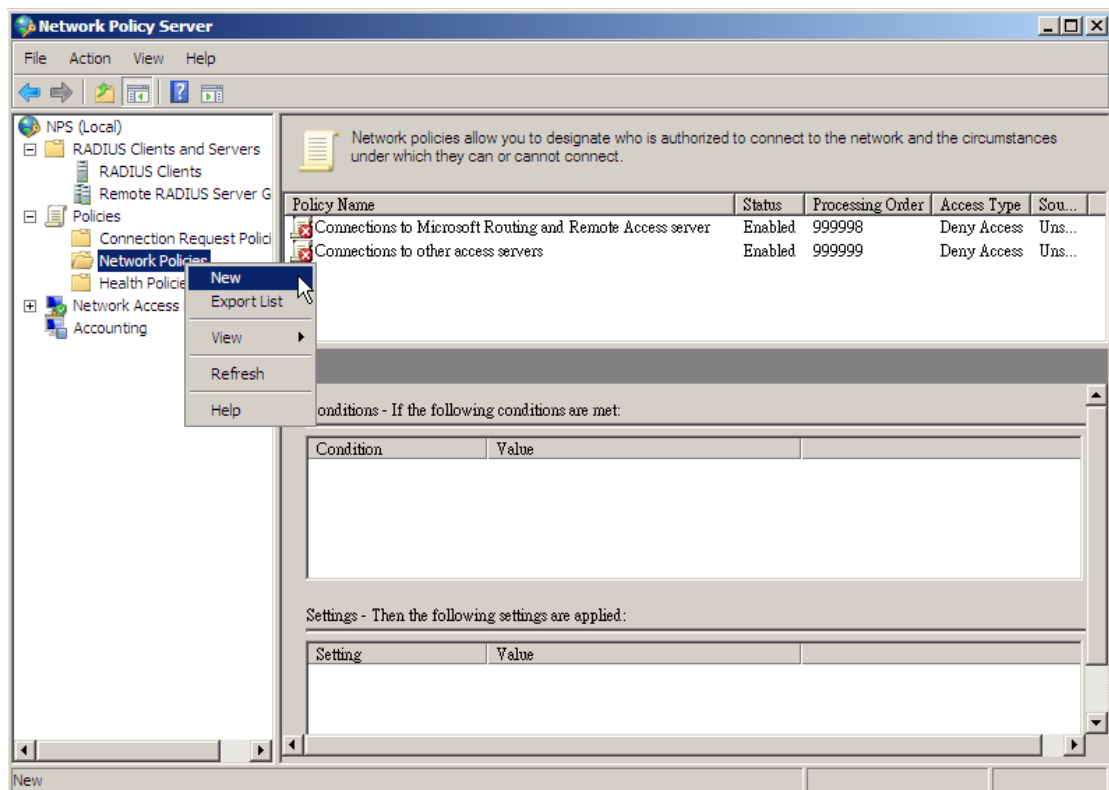
☐ RADIUS client is NAP-capable

OK Cancel

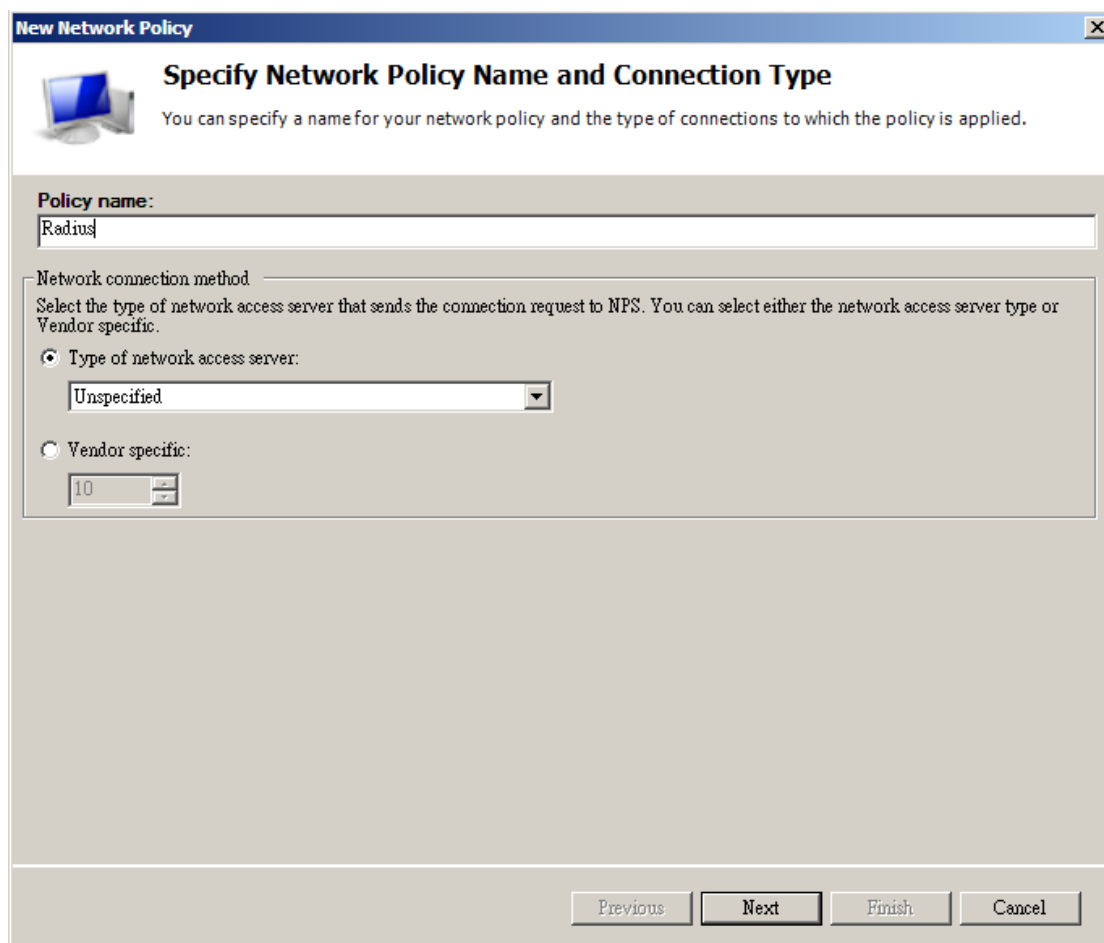
Adding a RADIUS Client




RADIUS Client Successfully Added



Adding a Network Policy



New Network Policy

 **Specify Network Policy Name and Connection Type**

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
Radius

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ **Type of network access server:**
Unspecified

☐ **Vendor specific:**
10

Previous Next Finish Cancel

Specifying the Policy Name and Connection Type

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:






Condition	Value

Condition description:

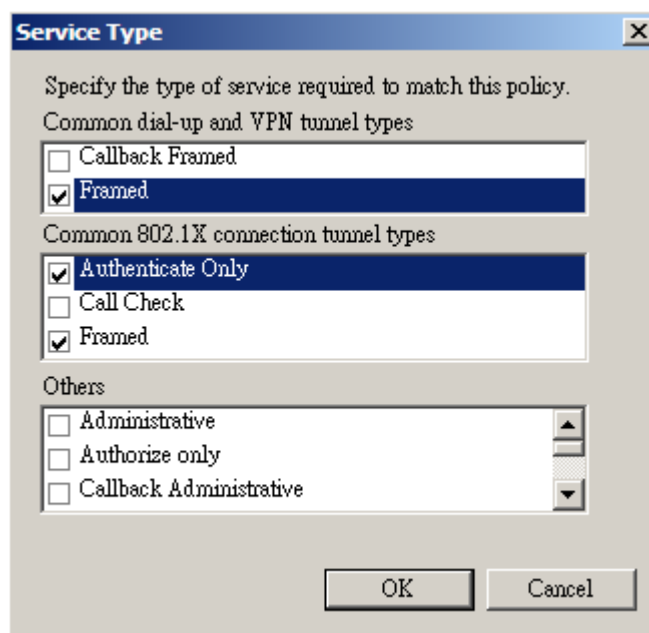
Adding a Condition

Select condition

Select a condition, and then click Add.

-  **Framed Protocol**
The Framed Protocol condition restricts the policy to only clients specifying a certain framing protocol for incoming packets, such as PPP or SLIP.
-  **Service Type**
The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.
-  **Tunnel Type**
The Tunnel Type condition restricts the policy to only clients that create a specific type of tunnel, such as PPTP or L2TP.
- RADIUS Client
-  **Calling Station ID**
The Calling Station ID condition specifies the network access server telephone number dialed by the access client.
-  **Client Friendly Name**
The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connection request to NPS.

Scrolling Down to Select Service Type



Service Type

Specify the type of service required to match this policy.

Common dial-up and VPN tunnel types

☐ Callback Framed

☒ Framed

Common 802.1X connection tunnel types

☒ Authenticate Only

☐ Call Check

☒ Framed

Others

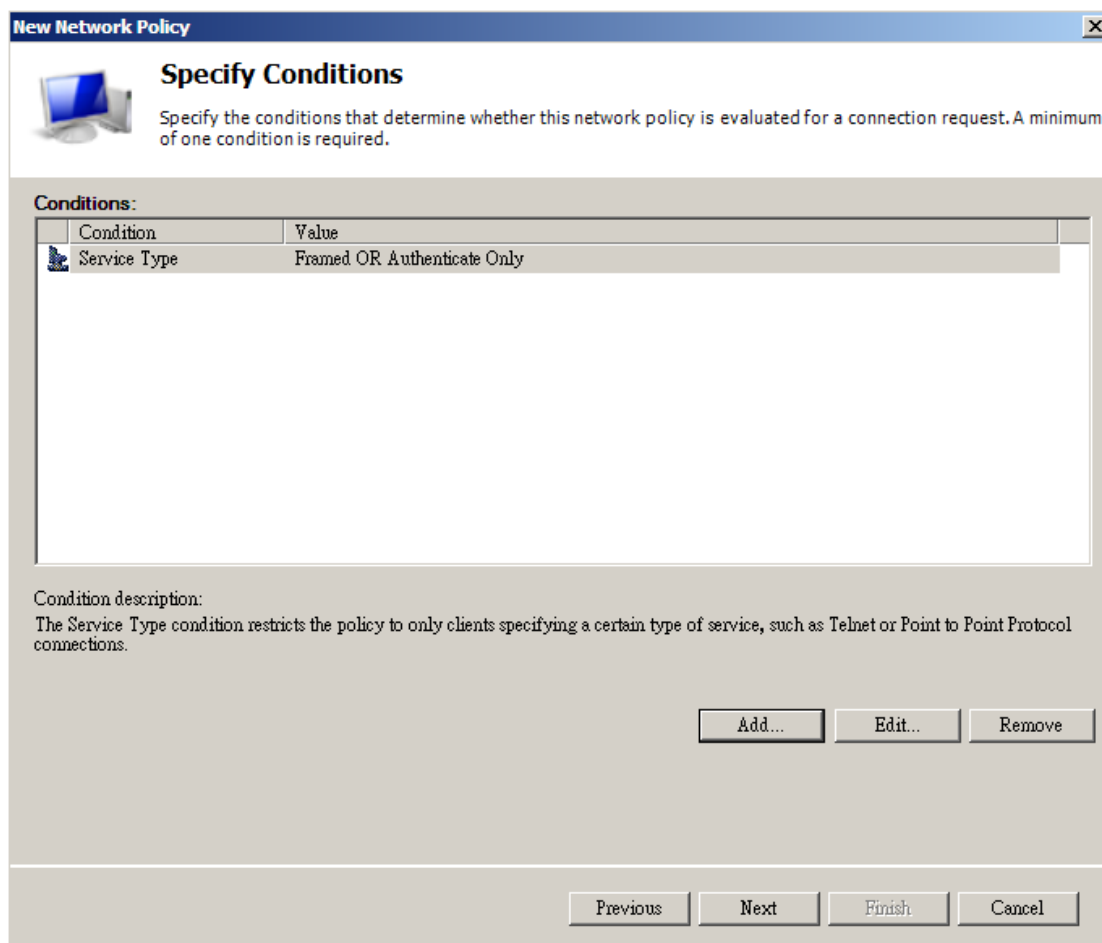
☐ Administrative

☐ Authorize only

☐ Callback Administrative

OK Cancel

Selecting the Service Types




New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
 Service Type	Framed OR Authenticate Only


Condition description:
The Service Type condition restricts the policy to only clients specifying a certain type of service, such as Telnet or Point to Point Protocol connections.

Add... Edit... Remove

Previous Next Finish Cancel

Policy Conditions Successfully Specified

New Network Policy

 **Specify Access Permission**

Configure whether you want to grant network access or deny network access if the connection request matches this policy.


☒ **Access granted**
Grant access if client connection attempts match the conditions of this policy.

☐ **Access denied**
Deny access if client connection attempts match the conditions of this policy.

☐ **Access is determined by User Dial-in properties (which override NPS policy)**
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Granting the Access Permission

New Network Policy

 **Configure Authentication Methods**

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- ☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☐ User can change password after it has expired
- ☒ Microsoft Encrypted Authentication (MS-CHAP)
 - ☐ User can change password after it has expired
- ☒ Encrypted authentication (CHAP)
- ☒ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous Next Finish Cancel

Selecting Authentication Methods

New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout**
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

Previous Next Finish Cancel

Configuring Constraints If Needed

Attribute Information

Attribute name:
Framed-Protocol

Attribute number:
7

Attribute format:
Enumerator

Attribute Value:
☒ Commonly used for Dial-Up or VPN
PPP

☐ Others
<none>

OK Cancel

Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:
☒ Commonly used for Dial-Up or VPN
Framed

☐ Commonly used for 802.1x
<none>

☐ Others
<none>

OK Cancel

Changing the RADIUS Attribute Values

New Network Policy
✕

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- Standard
- ☐ Vendor Specific

Network Access Protection

- NAP Enforcement
- Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add...
Edit...
Remove

Previous
Next
Finish
Cancel

RADIUS Attribute Values Successfully Changed

New Network Policy
✕

Completing New Network Policy

You have successfully created the following network policy:

Radius

Policy conditions:

Condition	Value
Service Type	Framed OR Authenticate Only

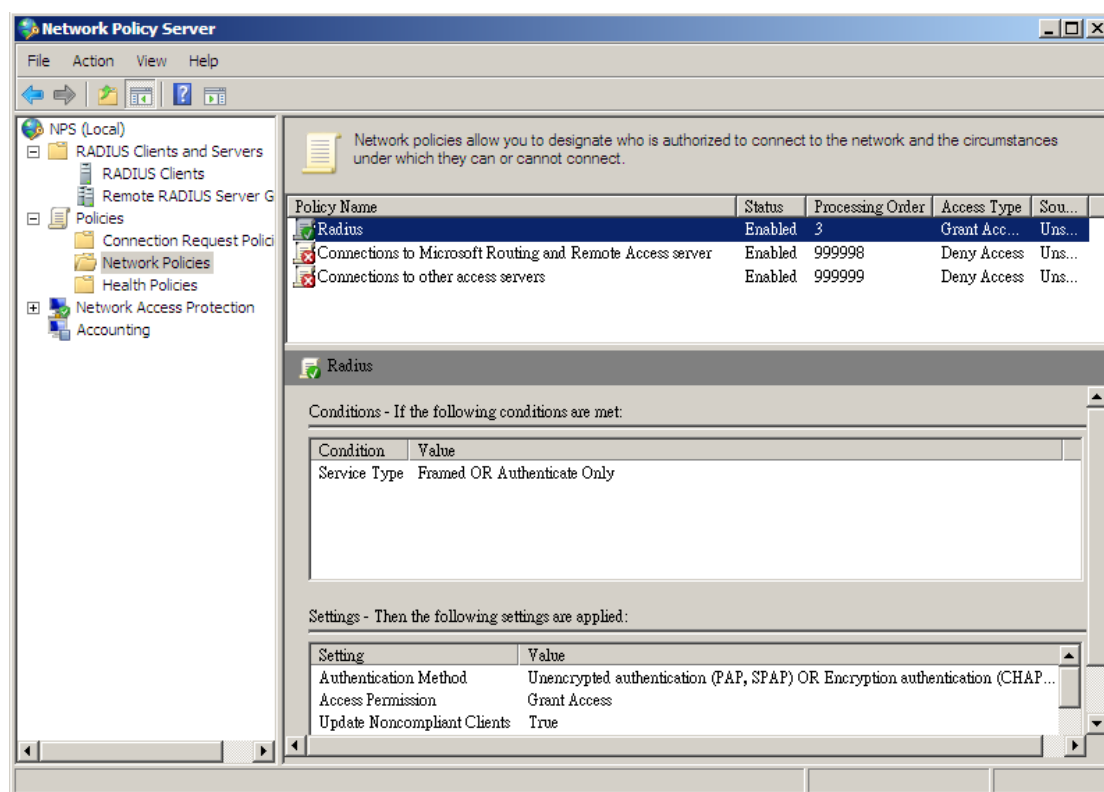
Policy settings:

Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 ...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

Previous
Next
Finish
Cancel

Confirming the Policy Settings

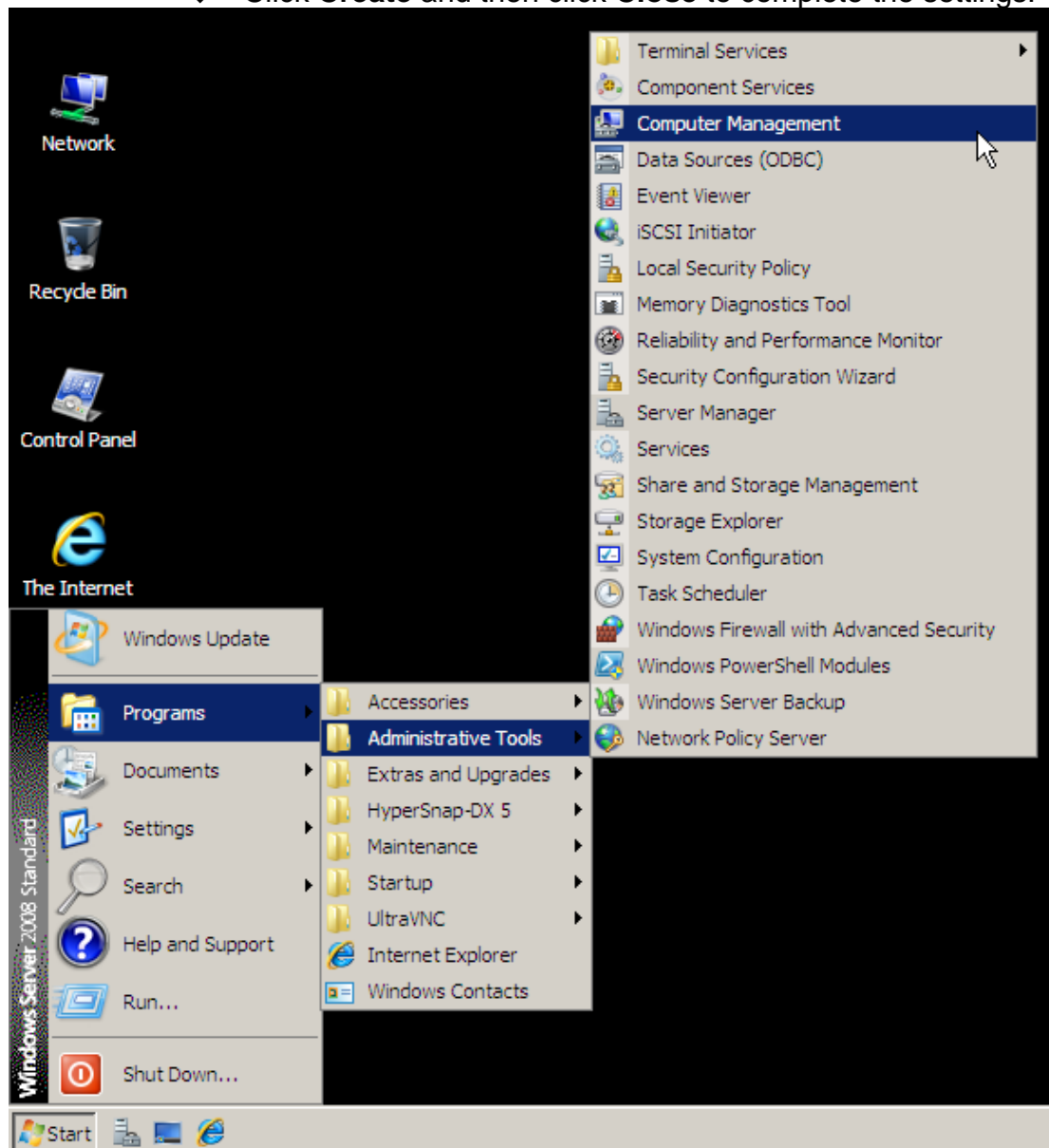


Network Policy Successfully Added

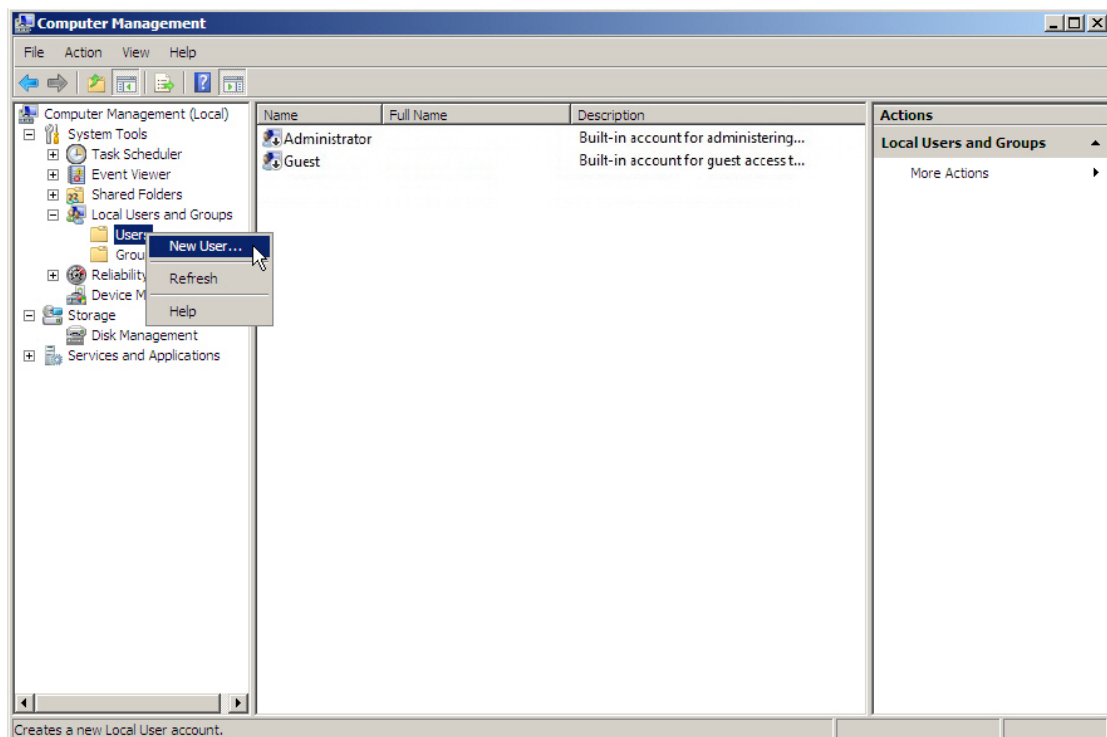
Step 3. Go to **Start > Programs > Administrative Tools > Computer Management** and then set as shown below:

- In the **Computer Management (Local)** tree panel, expand **System Tools**, expand **Local Users and Groups**, right-click **Users**, and then select **New User**.

- In the **New User** dialog box, set as shown below:
 - ◆ Specify a user name and a password.
 - ◆ Tick the box of "Password never expires".
 - ◆ Click **Create** and then click **Close** to complete the settings.



Selecting the Computer Management on the Start Menu



Selecting the New User from the Shortcut Menu

New User

User name: jackie

Full name:

Description:

Password:

Confirm password:

☐ User must change password at next logon

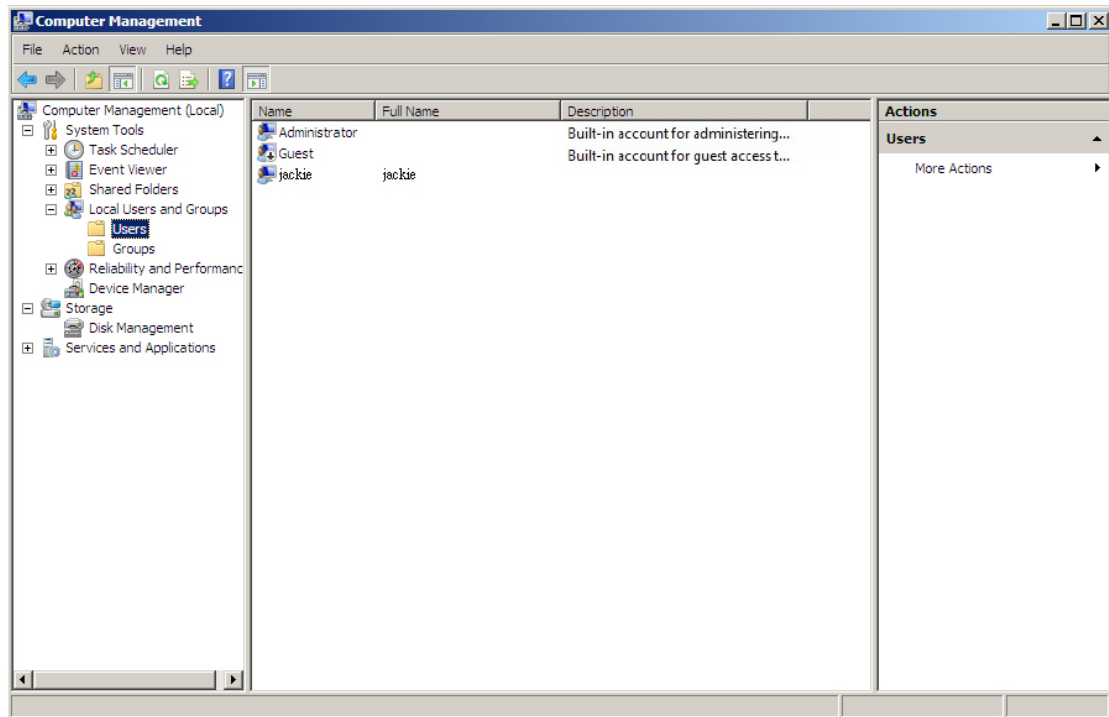
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

Help Create Close

Adding a User



User Successfully Added

Step 4. Under **Policy Object > Authentication > RADIUS**, configure the **RADIUS Server Settings** according to your Windows 2008 RADIUS server:

RADIUS Server Settings

☒ Enable RADIUS server authentication [Test connection](#)


RADIUS Server IP or Hostname : (Max. 80 characters)

RADIUS Server Port : (1025 - 65535, ex. 1812)

RADIUS Server Shared Secret : (Max. 80 characters)

☐ Enable 802.1x RADIUS server authentication

Configuring the RADIUS Server Settings

- 
Note

1. You may click **Test Connection** to test the connection to your RADIUS server.
 2. **RADIUS account** lists the accounts that are obtained from RADIUS server. The accounts can be grouped for the purpose of authentication accordingly.

Step 5. Under **Policy Object > Authentication > Group**, select as shown below:

Add Auth Group

Group Name : (Max. 20 characters)

===== [Available Accounts] =====

(POP3 Server)
(LDAP Server)

===== [Applied Accounts] =====

(RADIUS Server)

The Group Setting for User Authentication

Step 6. Under **Policy > Outgoing**, set as shown below:

- Select the authentication group for **Authentication**.
- Click **OK** to complete the settings.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (WAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☒ Enabled

Traffic Grapher : ☒ Enabled

Web Filter :

Application Blocking :

Creating a Policy to Apply the Authentication Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any			Modify Remove Pause	1

[New Entry](#)

Policy Successfully Created

Step 7. The group members will be prompted for their authentication credentials to access the Internet. Click **Login** to complete the authentication procedure.

User Authentication - Login

Username :

Password :

[Login](#)

The Authentication Prompt Screen

4.5.3 POP3 Authentication

4.5.3.1 Managing Internet Access with a POP3 Server


Step 1. Under **Policy Object > Authentication > POP3**, set as shown below:

Add POP3 Server

POP3 Server IP or Hostname : (Max. 80 characters)
POP3 Server Port : (1 - 65535, ex. 110 or 995)
☐ Enable domain name filtering (Max. 80 characters)
☐ Enable SSL support
POP3 Server Connection Test : [Test Connection](#) [Help](#)

[OK](#) [Cancel](#)

Adding a POP3 Server



Note

1. You may click **Test Connection** to test the connection to your POP3 Server.
2. To designate the domain name that connects to the POP3 server, tick **Enable domain name filtering**.
3. To process the authentication using POP3s protocol, tick **Enable SSL support**.

Step 2. Go to **Policy Object > Authentication > Group** and then set as shown below:

Add Auth Group

Group Name : (Max. 20 characters)

===== [Available Accounts] =====
(RADIUS Server)
(LDAP Server)

===== [Applied Accounts] =====
(POP3 Server)

The Group Setting for User Authentication

Step 3. Under **Policy > Outgoing**, set as shown below:

- **Authentication:** Select the authentication group.
- Click **OK** to complete the settings.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

☒ Permit All ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (WAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

Application Blocking :

☐ Advanced Settings

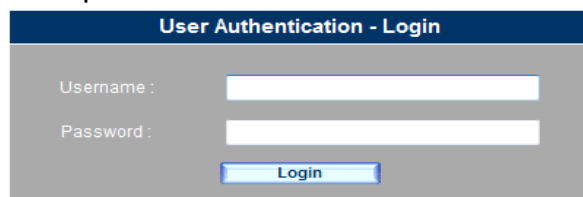
Creating a Policy to Apply the Authentication Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any			Modify Remove Pause	1

[New Entry](#)

Policy Successfully Created

Step 4. The group members will be prompted for their authentication credentials to access the Internet. Click **Login** to complete the authentication procedure.



The screenshot shows a login window titled "User Authentication - Login". It contains two input fields: "Username :" and "Password :". Below these fields is a blue button labeled "Login".

The Authentication Prompt Screen

4.5.4 LDAP Authentication

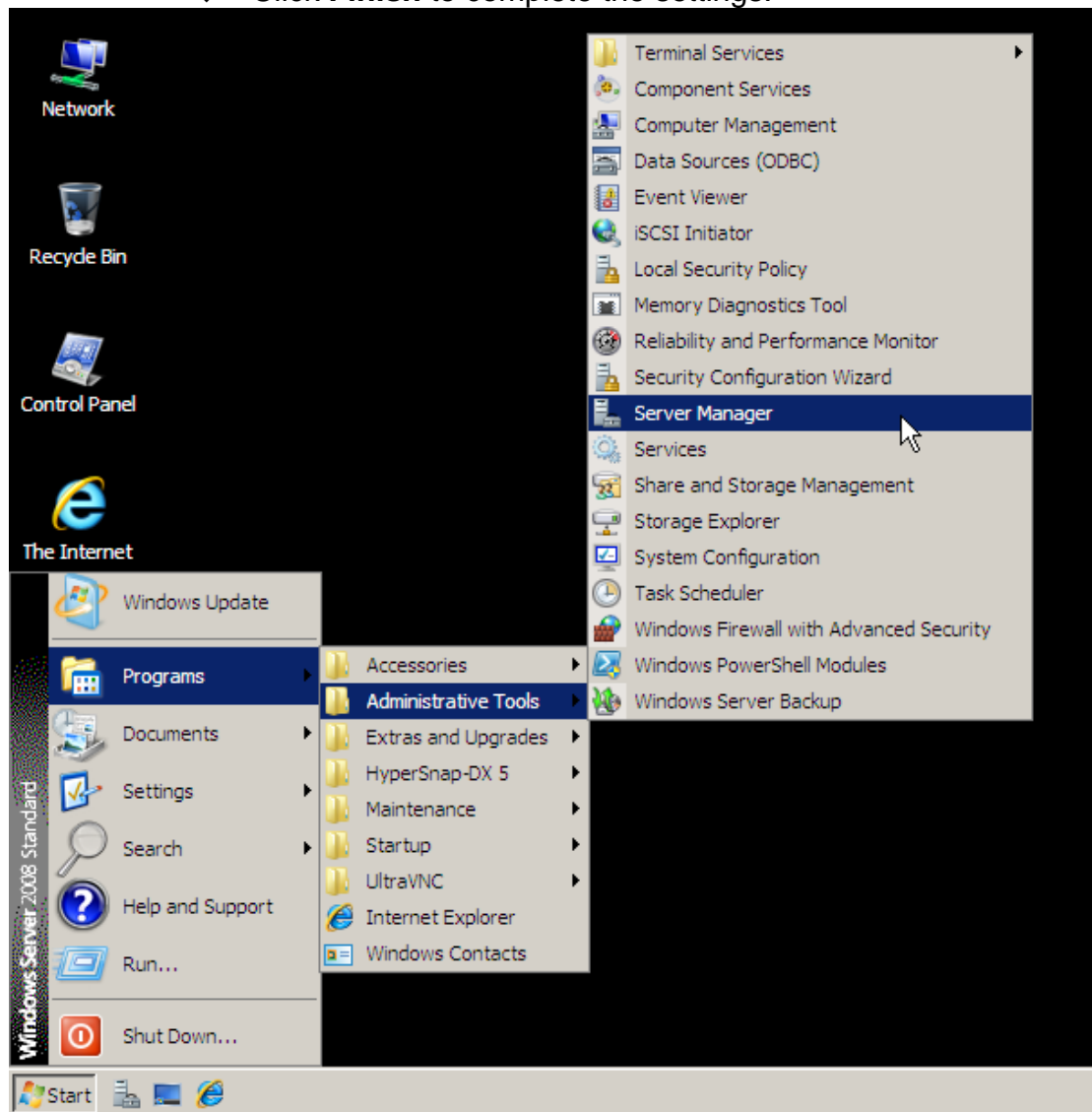
4.5.4.1 Managing Internet Access with a Windows 2008 LDAP Server

※ Setting up a Windows 2008 LDAP Server

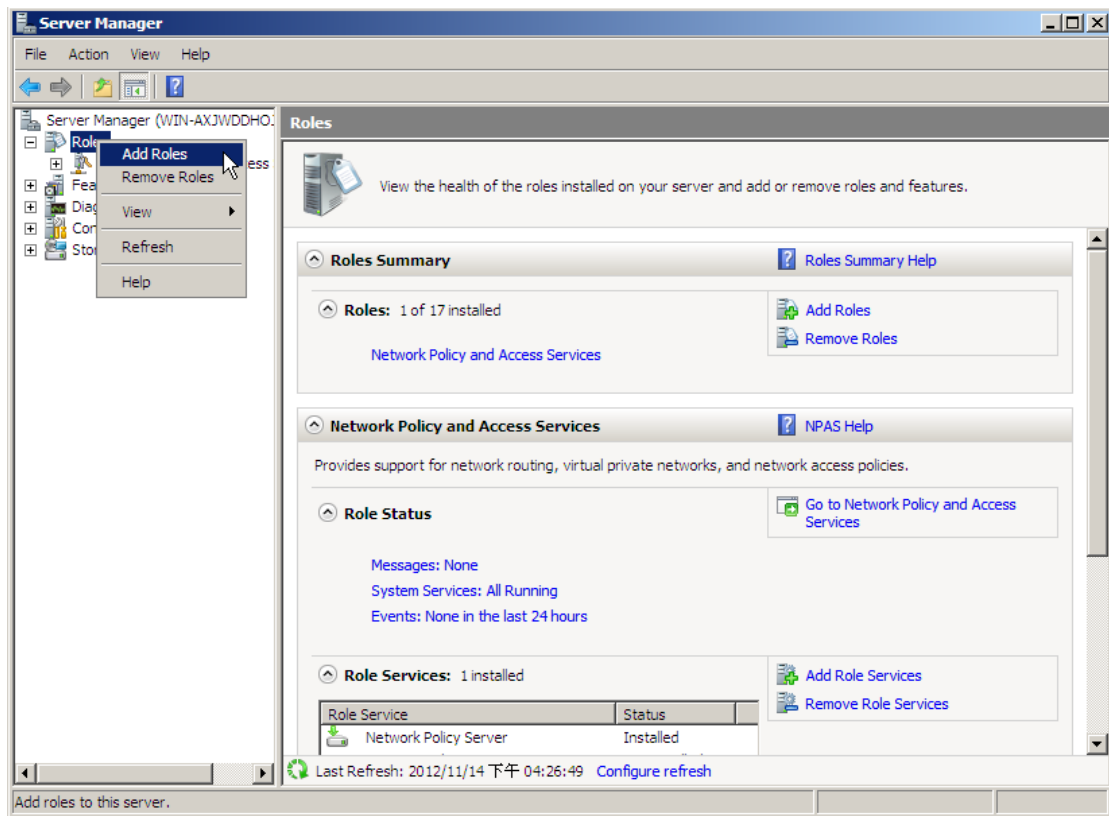
Step 1. Go to **Start > Programs > Administrative Tools > Server Manager** and then set as shown below:

- In the **Server Manager** tree panel, right-click **Roles** and then select **Add Roles**.
- In the **Add Roles Wizard** dialog box, set as shown below:
 - ◆ Tick the box of "Active Directory Domain Services" under the **Roles** section.
 - ◆ Click **Next**.
 - ◆ Click **Next**.
 - ◆ Click **Install**.
 - ◆ Click **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)**.
- In the **Active Directory Domain Services Installation Wizard** dialog box, set as shown below:
 - ◆ Click **Next**.
 - ◆ Click **Next**.
 - ◆ Select the radio box of "Create a new domain in a new forest".
 - ◆ Click **Next**.
 - ◆ **FQDN of the forest root domain:** Type in "my.com".
 - ◆ Click **Next**.
 - ◆ **Forest functional level:** Select "Windows Server 2008".
 - ◆ Click **Next**.
 - ◆ Tick the box of "DNS server".

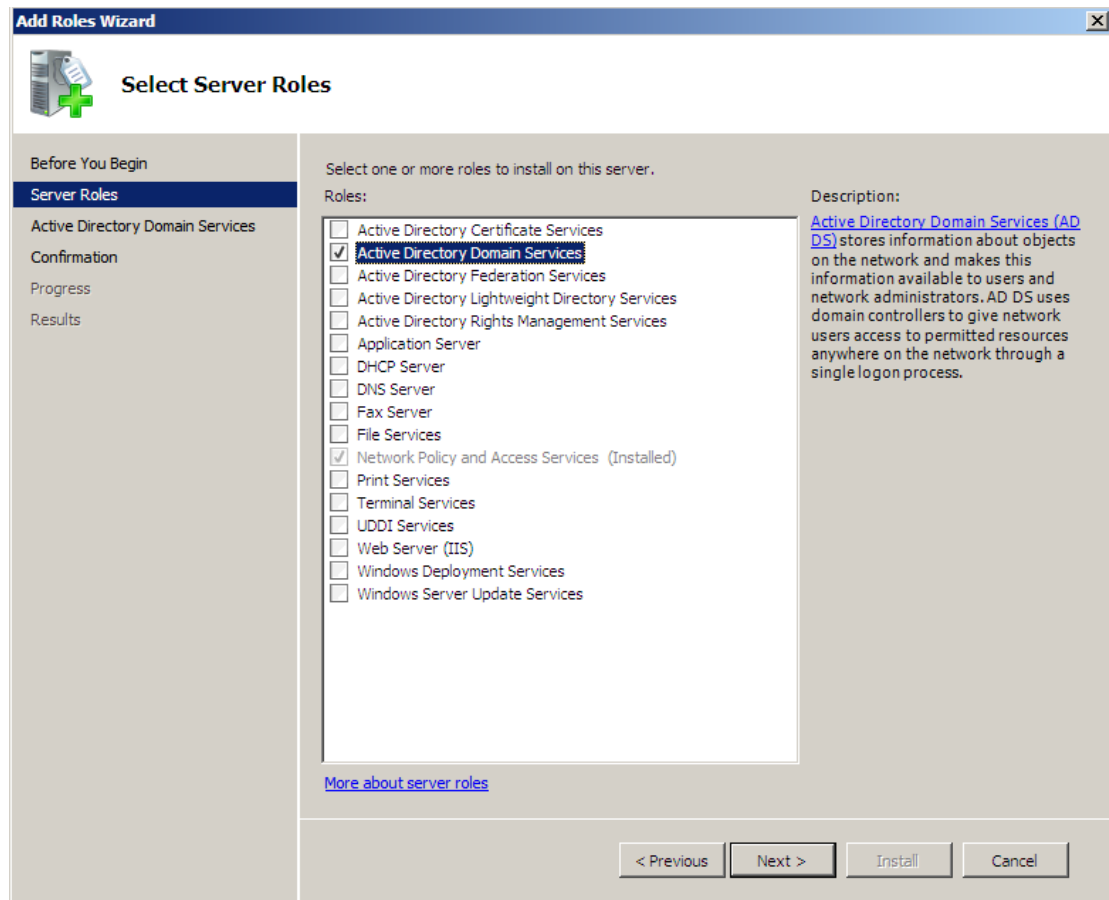
- ◆ Click **Next**
- ◆ Click **Next**
- ◆ Specify a password and repeat it to confirm.
- ◆ Click **Next**.
- ◆ Click **Next**.
- ◆ Click **Finish** to complete the settings.



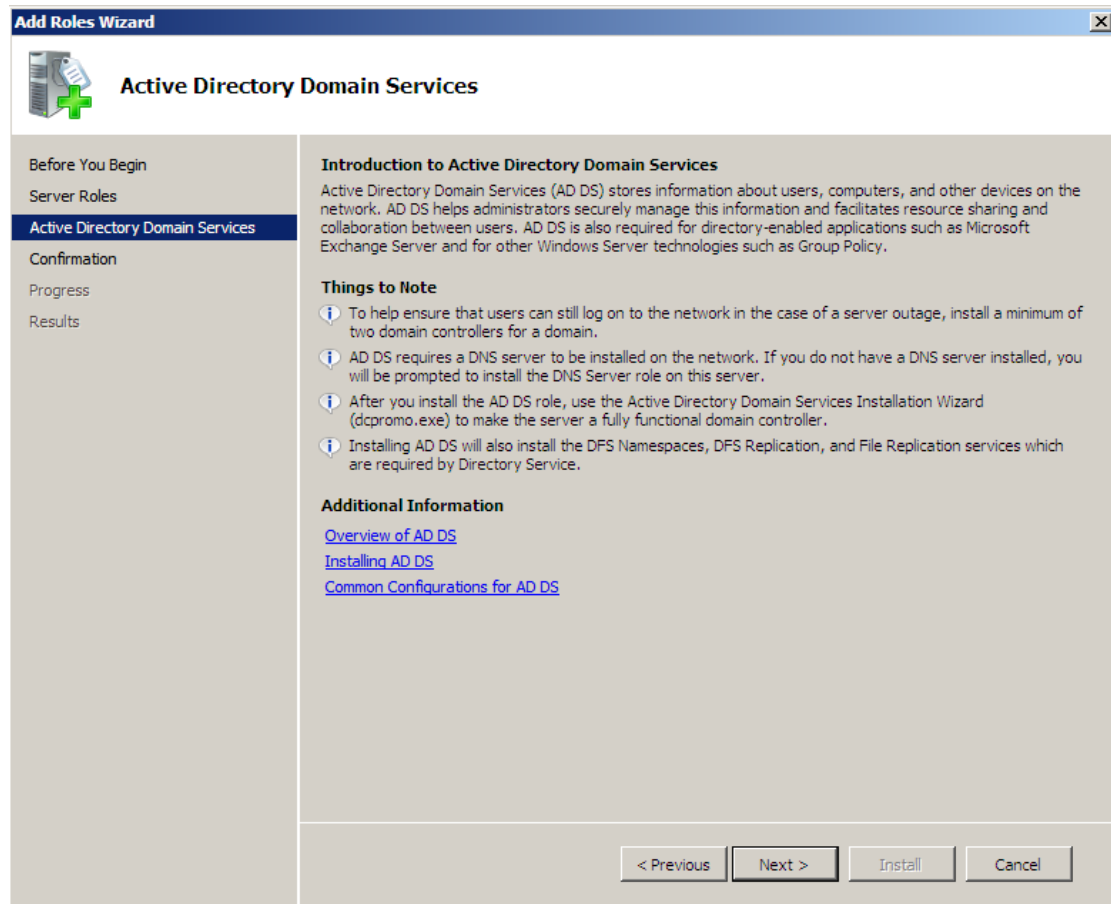
Selecting the Server Manager on the Start Menu



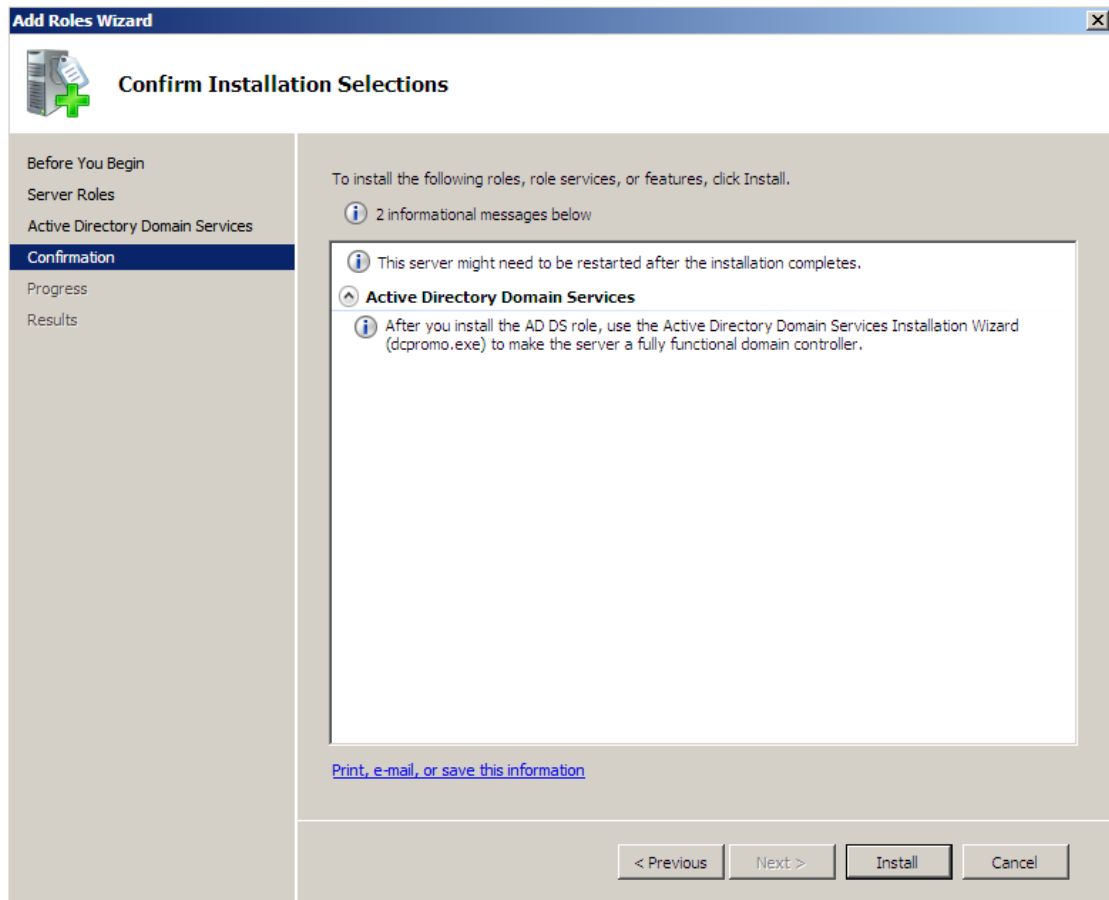
Adding a Role Service



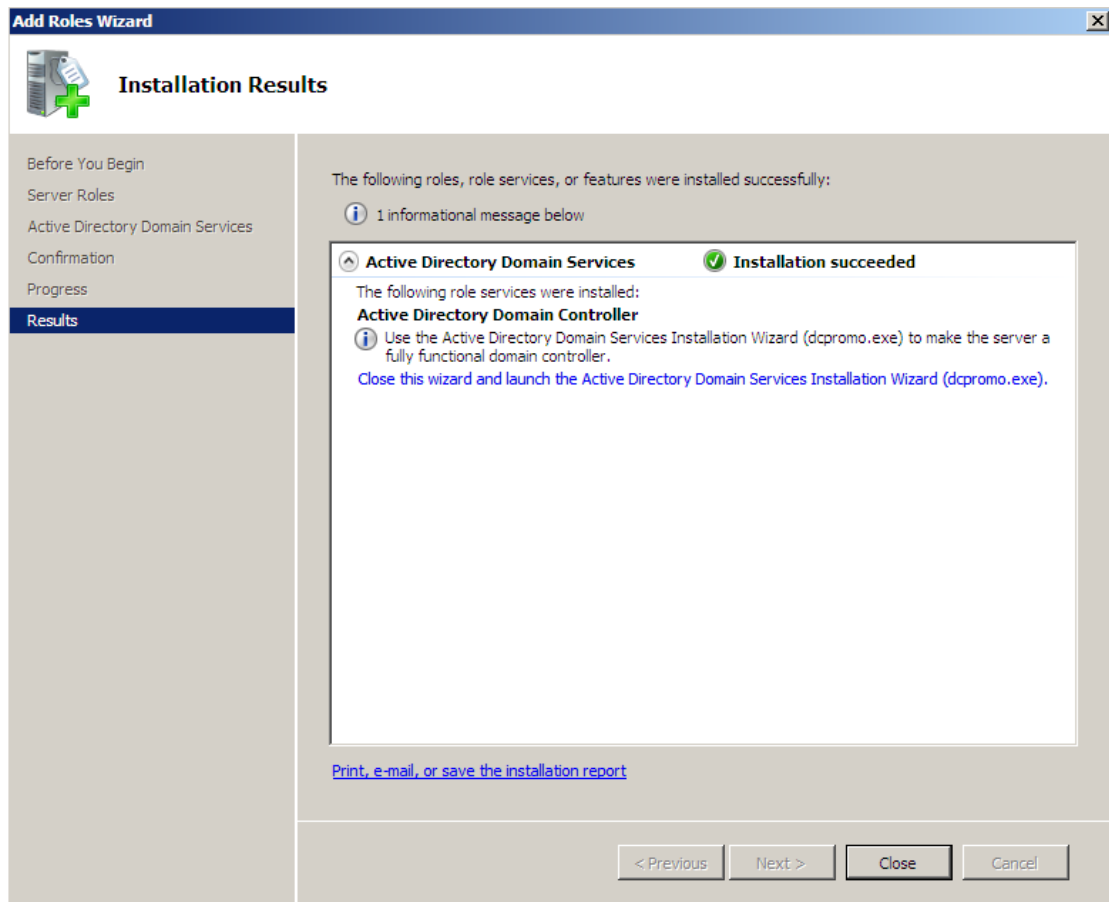
Selecting the Active Directory Domain Services



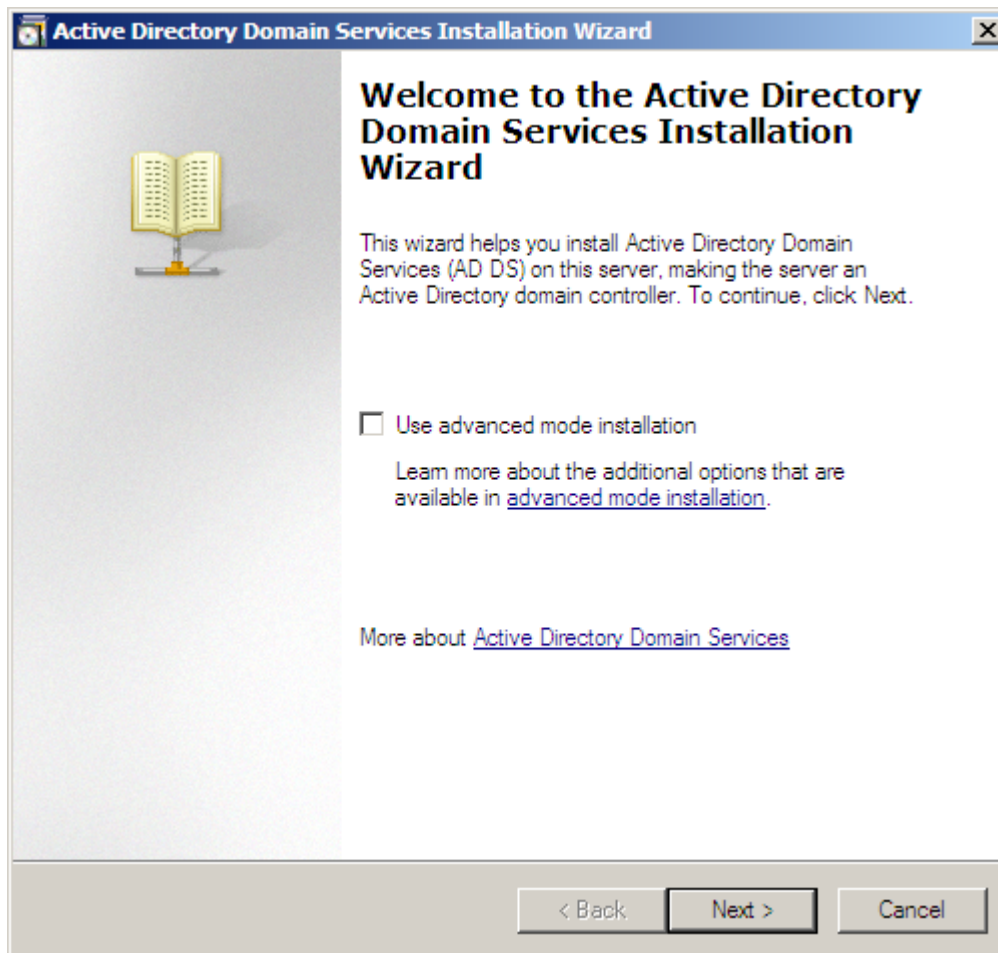
The Introduction to Active Directory Domain Services



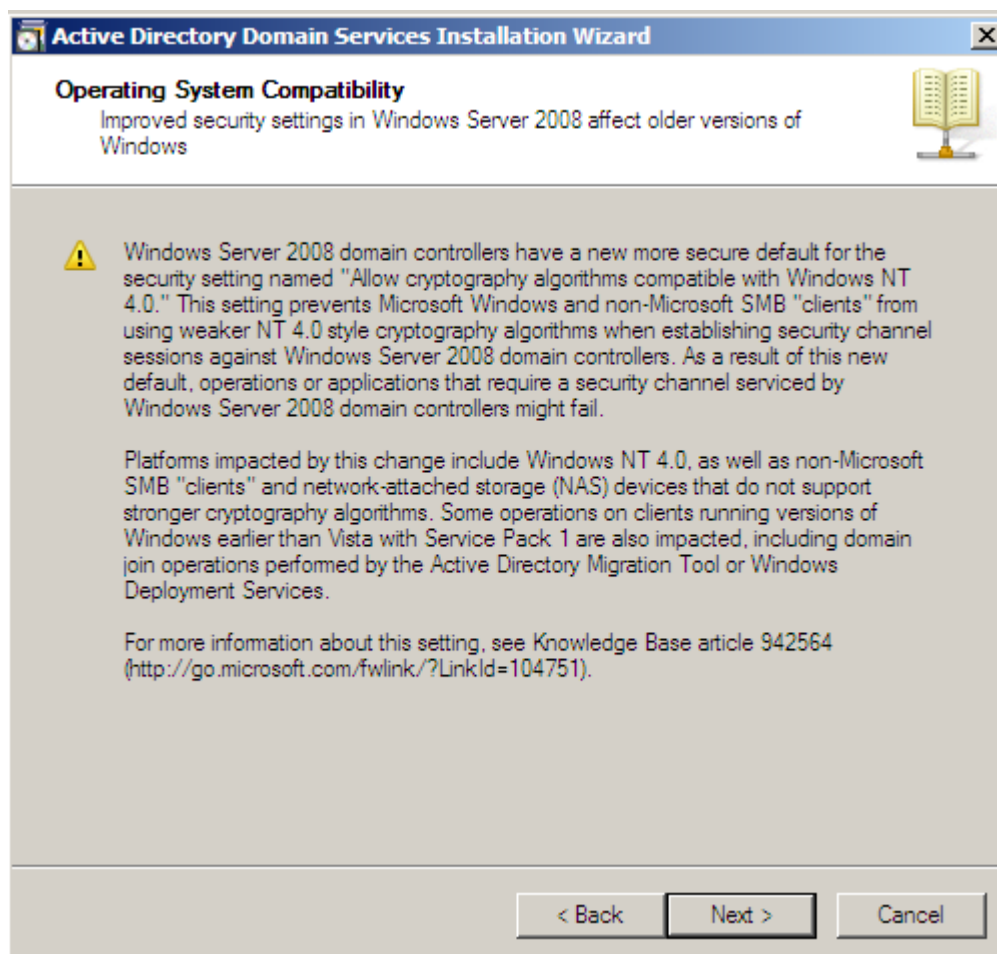
Confirming the Installation of Active Directory Domain Services



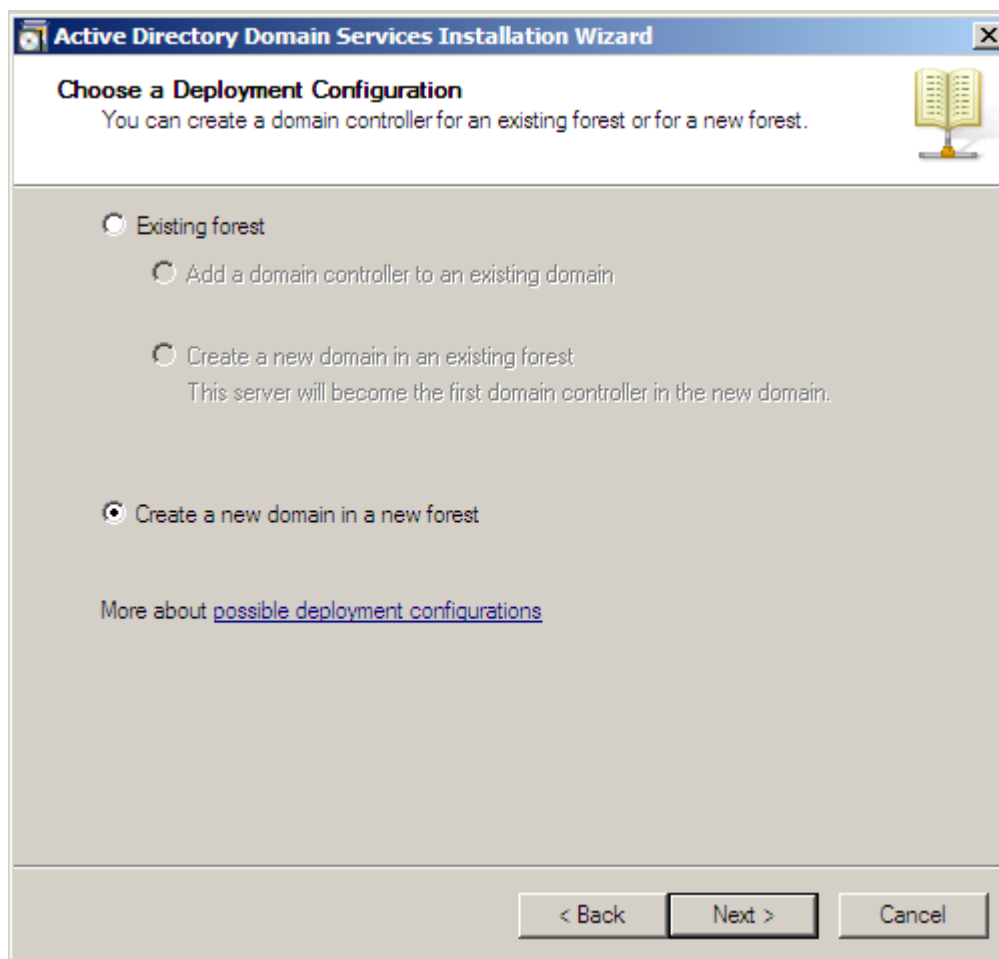
Launching the Active Directory Domain Services Installation Wizard



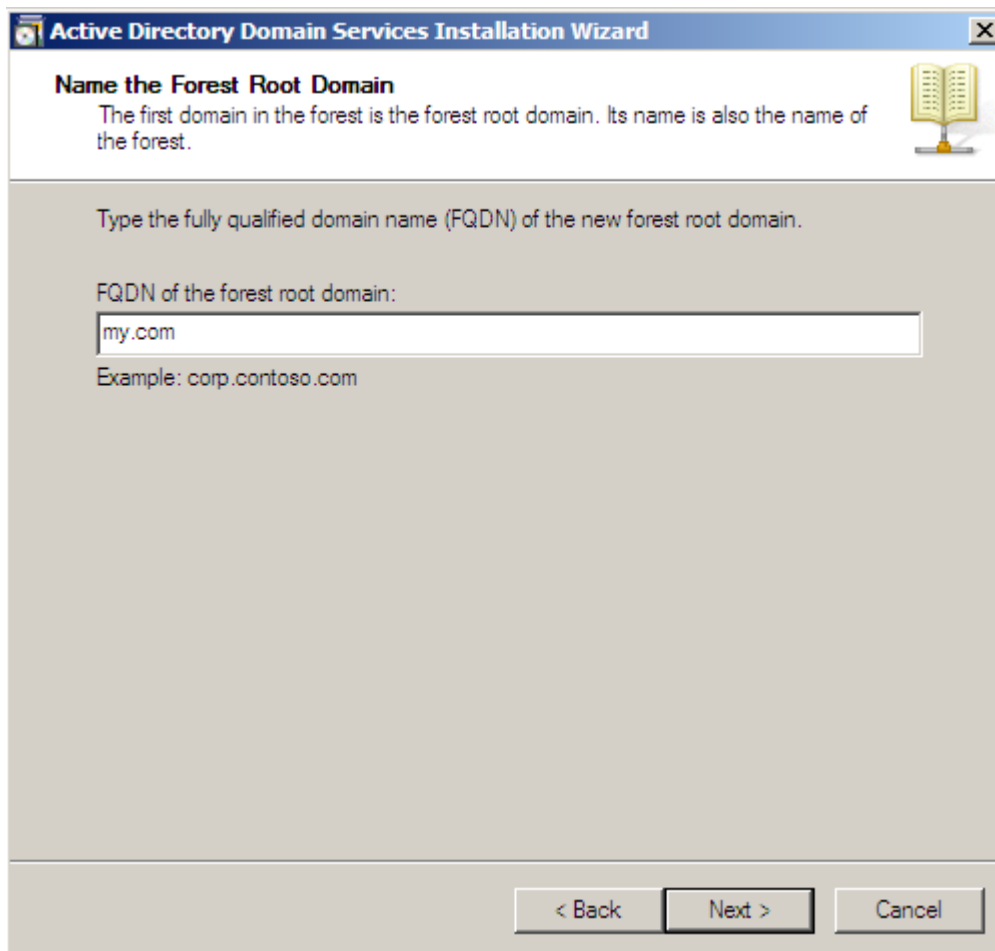
Active Directory Domain Services Installation Wizard



Operating System Compatibility



Choosing a Deployment Configuration



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Name the Forest Root Domain'. Below this, a text box explains: 'The first domain in the forest is the forest root domain. Its name is also the name of the forest.' To the right of this text is an icon of an open book. Below the explanation, a prompt says 'Type the fully qualified domain name (FQDN) of the new forest root domain.' This is followed by a label 'FQDN of the forest root domain:' and a text input field containing 'my.com'. Below the input field, an example is provided: 'Example: corp.contoso.com'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

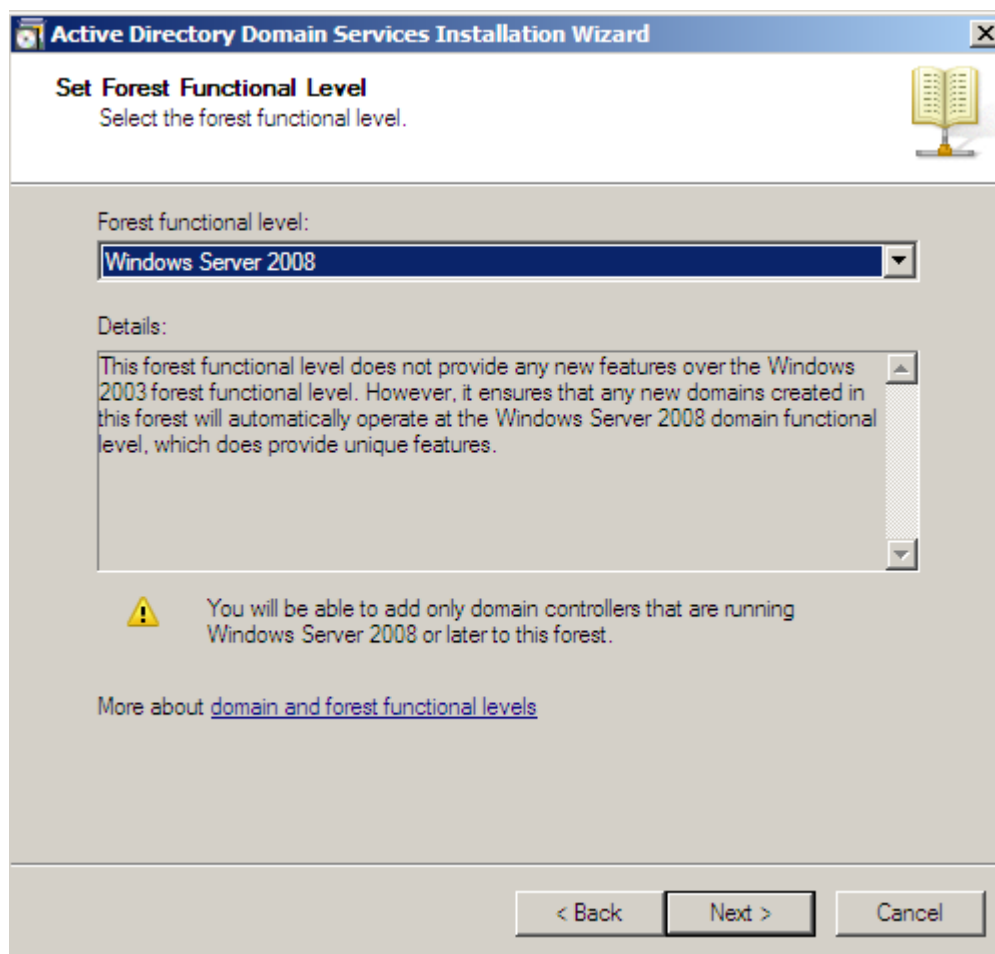
FQDN of the forest root domain:

my.com

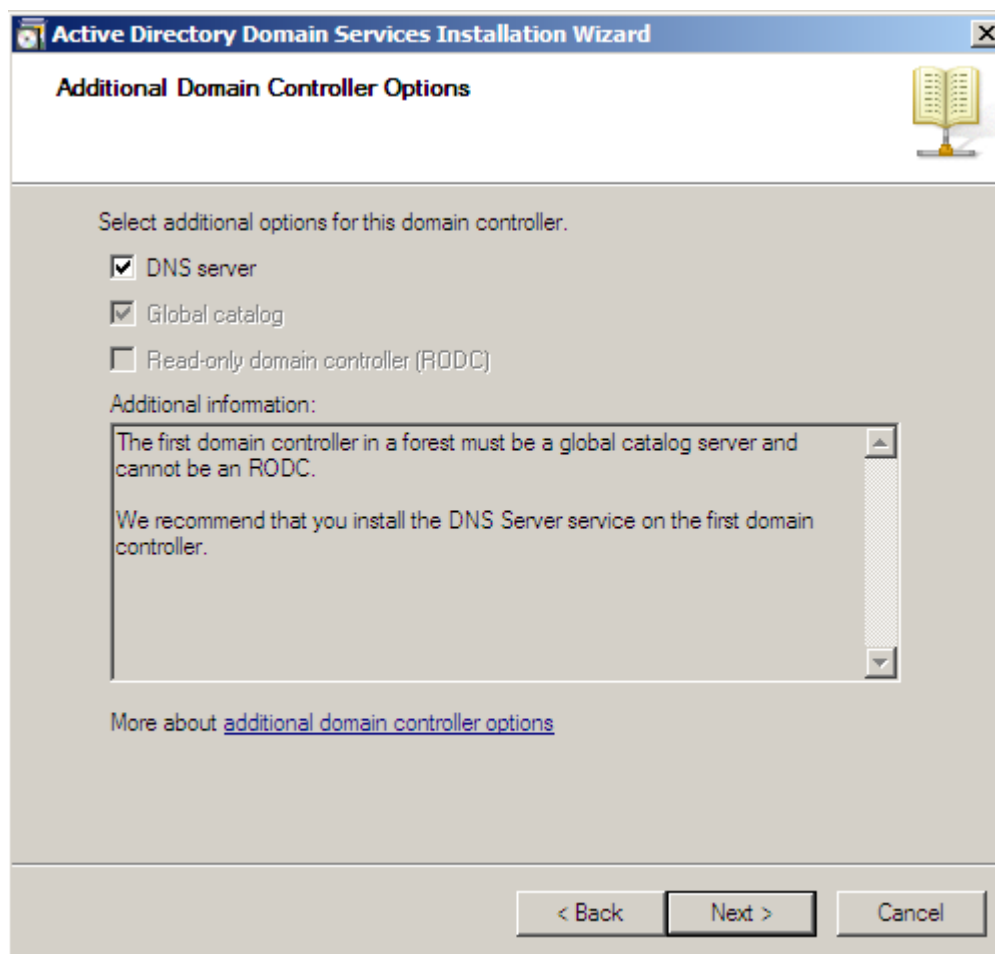
Example: corp.contoso.com

< Back Next > Cancel

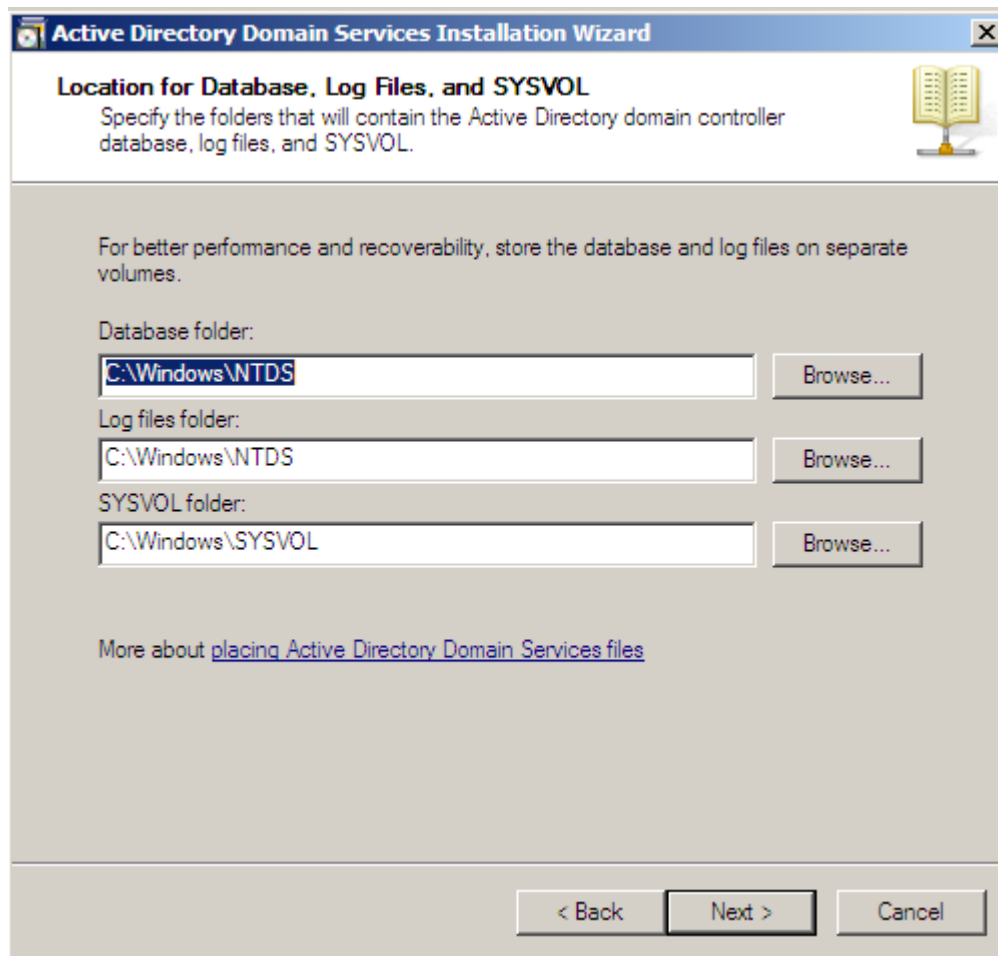
Naming the Forest Root Domain



Selecting the Forest Functional Level

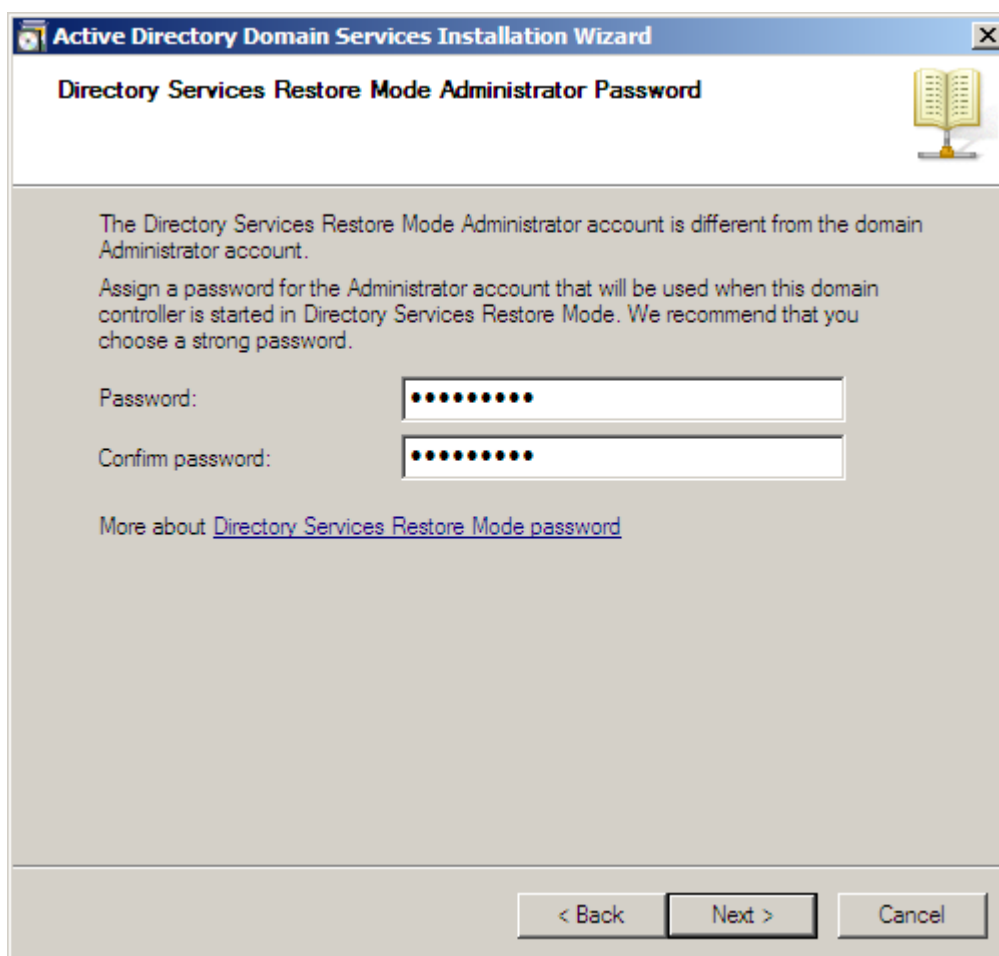


Selecting the DNS Server



The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Location for Database, Log Files, and SYSVOL'. Below this, it says 'Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.' There is a small icon of an open book to the right. A note states: 'For better performance and recoverability, store the database and log files on separate volumes.' Below this, there are three sections: 'Database folder:' with a text box containing 'C:\Windows\NTDS' and a 'Browse...' button; 'Log files folder:' with a text box containing 'C:\Windows\NTDS' and a 'Browse...' button; and 'SYSVOL folder:' with a text box containing 'C:\Windows\SYSVOL' and a 'Browse...' button. At the bottom left, there is a link: 'More about [placing Active Directory Domain Services files](#)'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Choosing the Location for Database, Log Files and SYSVOL



The screenshot shows a Windows XP-style window titled "Active Directory Domain Services Installation Wizard". The main heading is "Directory Services Restore Mode Administrator Password". To the right of the heading is a small icon of an open book. The text in the window explains that the Directory Services Restore Mode Administrator account is different from the domain Administrator account and instructs the user to assign a password for the Administrator account that will be used when the domain controller is started in Directory Services Restore Mode. It recommends choosing a strong password. Below the text are two input fields: "Password:" and "Confirm password:", both containing ten black dots. A blue hyperlink "More about [Directory Services Restore Mode password](#)" is located below the input fields. At the bottom right of the window are three buttons: "< Back", "Next >", and "Cancel".

Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

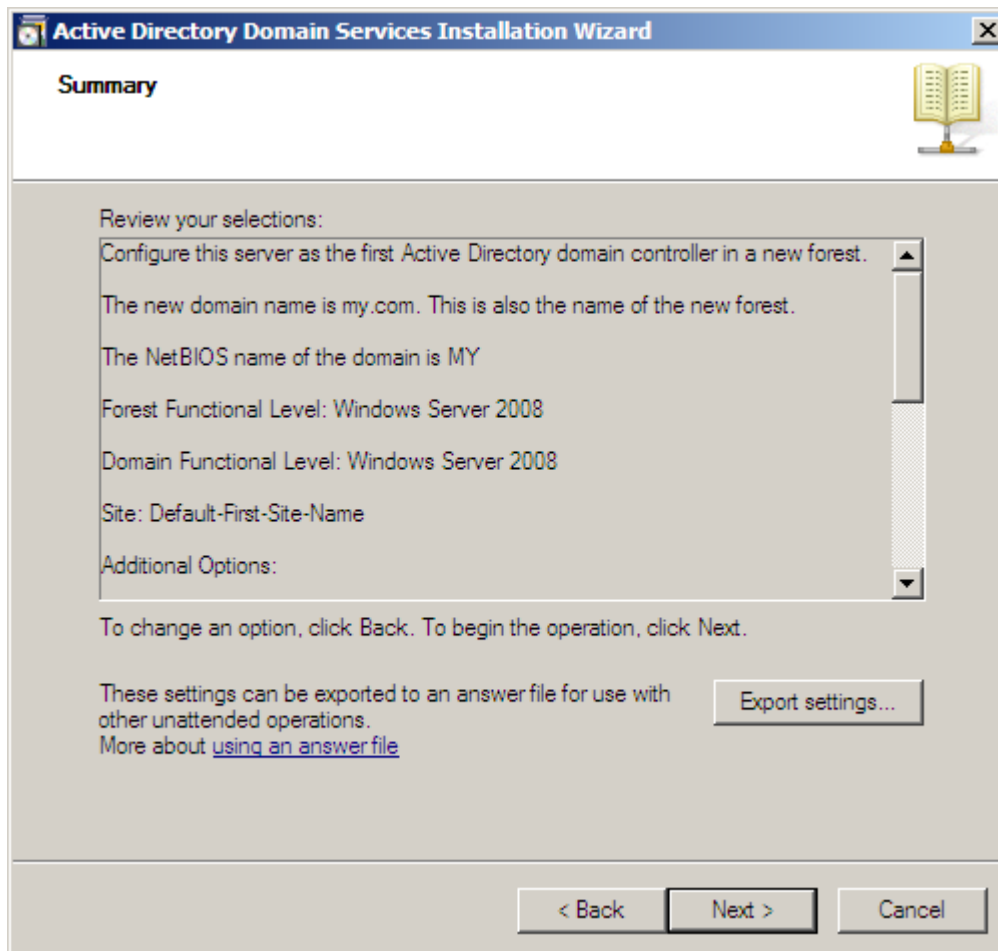
Password:

Confirm password:

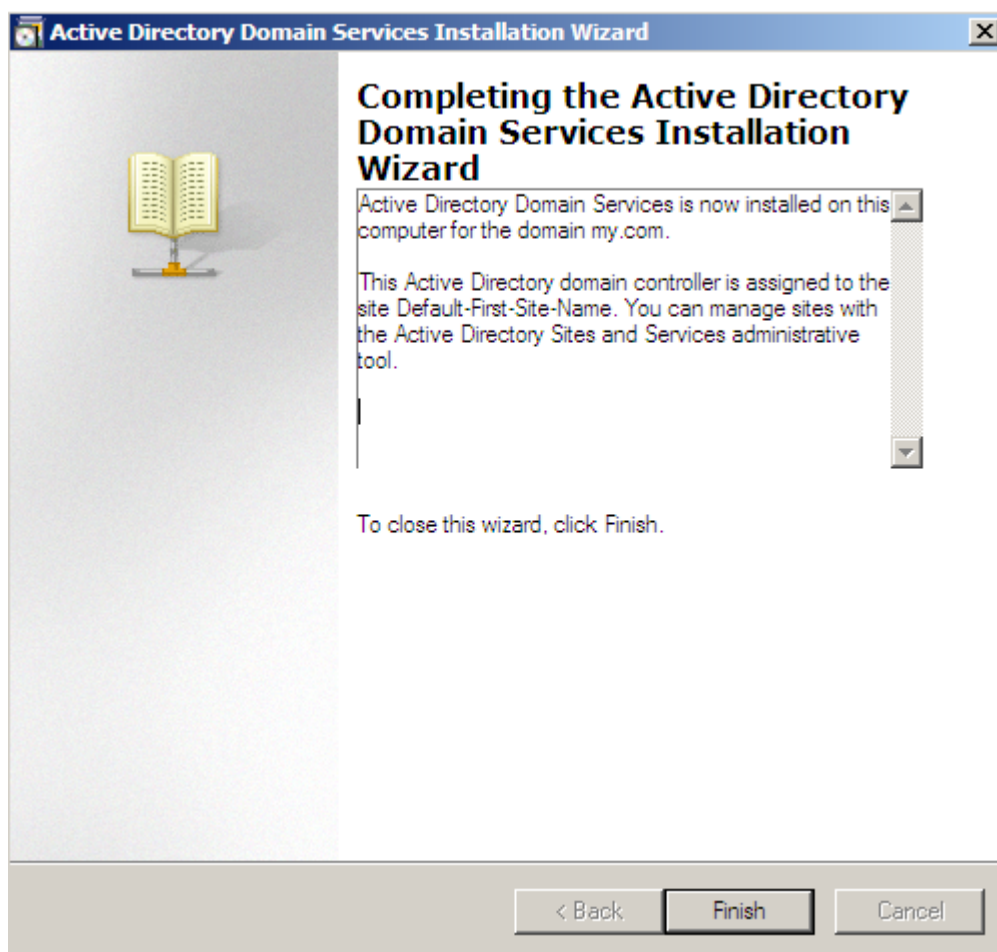
More about [Directory Services Restore Mode password](#)

< Back Next > Cancel

Specifying a Password for the Directory Services Restore Mode



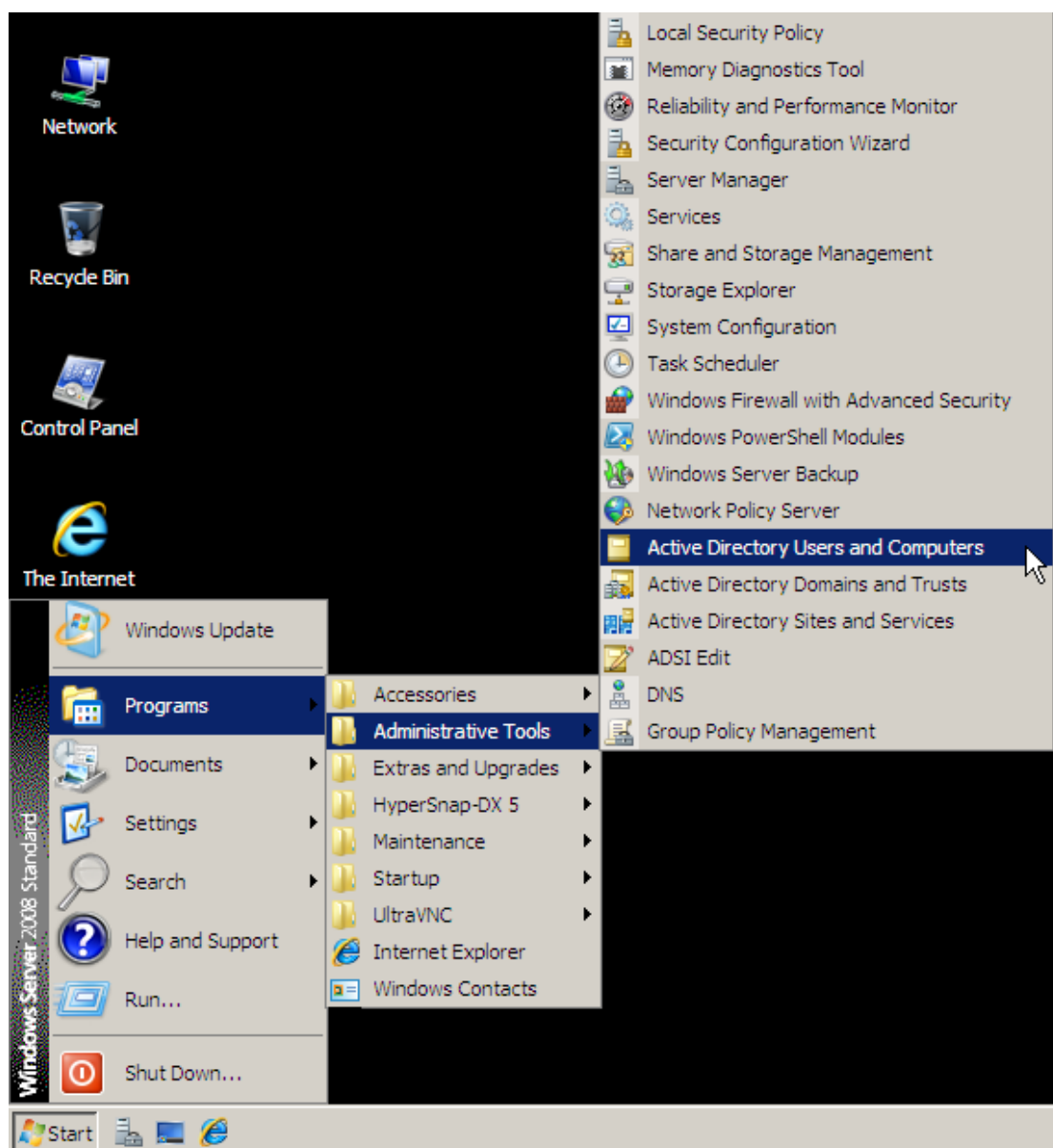
A Summary for Reviewing Your Selections



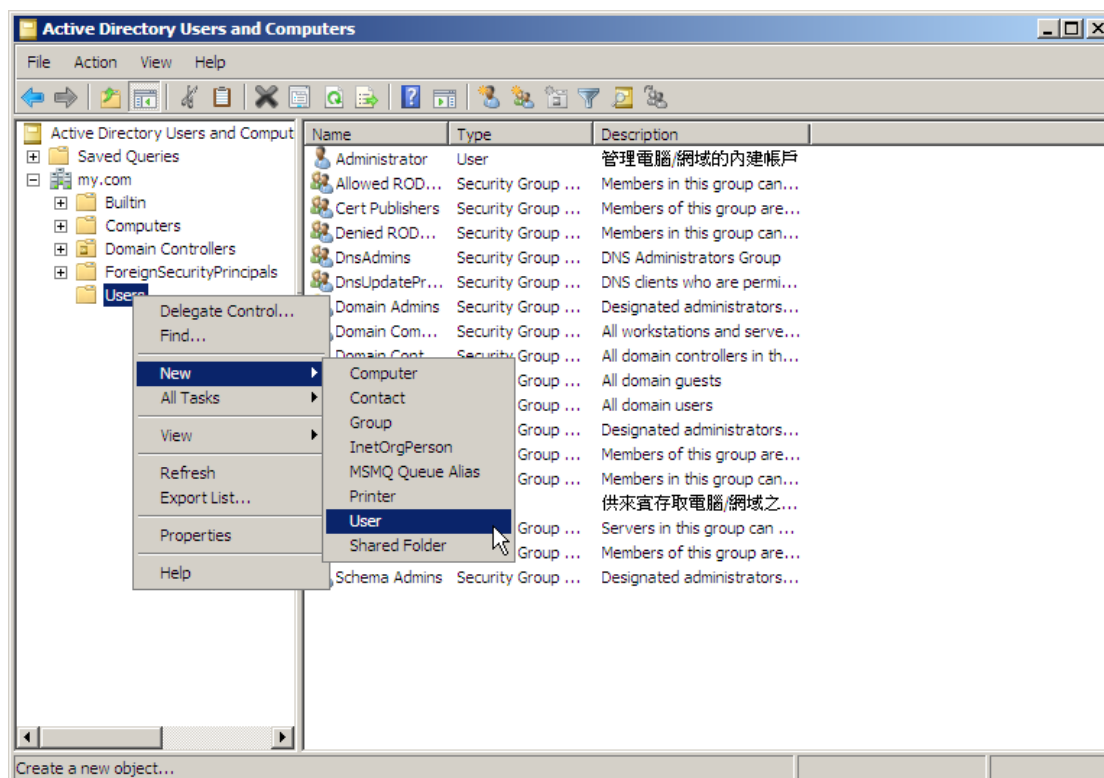
Completing the Active Directory Domain Services Installation

Step 2. Go to **Start > Programs > Administrative Tools > Active Directory Users and Computers** and then set as shown below:

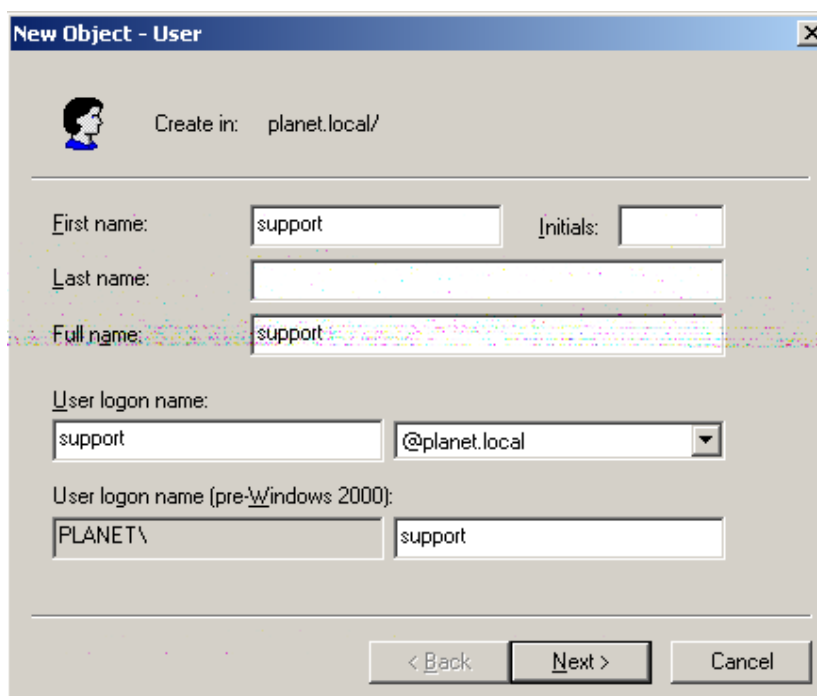
- In the **Active Directory Users and Computers** tree panel, expand **my.com** (or the name of your forest root domain), right-click **Users**, select **New**, and then select **User**.
- In the **New Object-User** dialog box, set as shown below:
 - ◆ Type in the **First name**, **Full name**, **User logon name** and **User logon name for pre-Windows 2000** respectively.
 - ◆ Click **Next**.
 - ◆ Specify a password and repeat it to confirm.
 - ◆ Tick the box of "Password never expires".
 - ◆ Click **Next**.
 - ◆ Click **Finish** to complete the settings.



Selecting the Active Directory Users and Computers on the Start Menu



Adding a New User



The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'planet.local/'. The 'First name' field contains 'support', and the 'Initials' field is empty. The 'Last name' field is empty. The 'Full name' field contains 'support'. The 'User logon name' field contains 'support', and the domain dropdown is set to '@planet.local'. The 'User logon name (pre-Windows 2000)' field contains 'PLANET\support'.

Create in: planet.local/

First name: support Initials:

Last name:

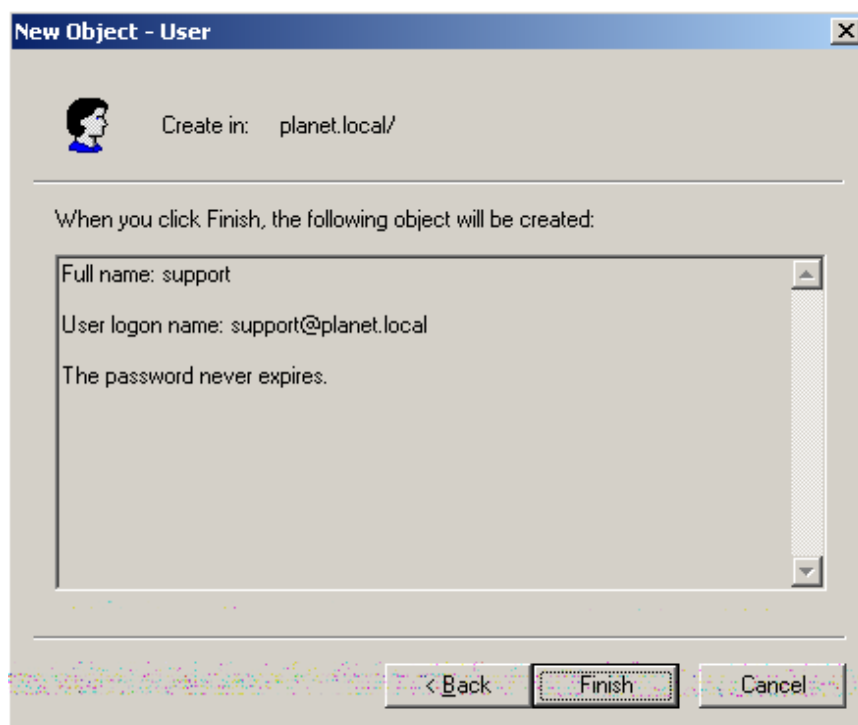
Full name: support

User logon name: support @planet.local

User logon name (pre-Windows 2000): PLANET\ support

< Back Next > Cancel

Typing in the User Information



Confirming the User Information

Step 3. Go to **Policy Object > Authentication > LDAP** and then set as shown below:

LDAP Server Settings

☒ Enable LDAP server authentication [Test Connection](#)

LDAP Server IP or Hostname : (Max. 80 characters)

LDAP Server Port : (1 - 65535, ex. 389)


LDAP Base DN : (Max. 1024 characters, ex. dc=mydomain, dc=com)

LDAP Bind DN : (Max. 1024 characters, ex. (objectClass=*))

Username : (Max. 1024 characters, ex. cn=account, cn=users, dc=mydomain, dc=com)

Password : (Max. 1024 characters)

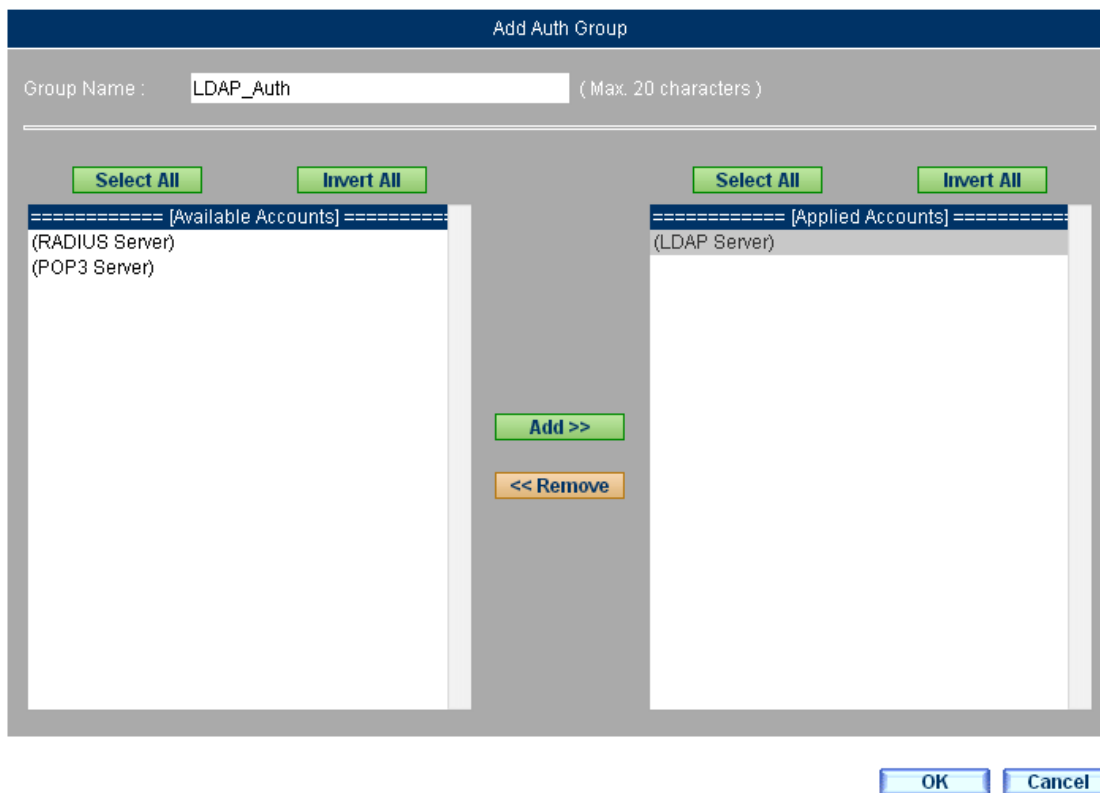
Configuring LDAP Server Settings

- 

Note

1. You may click **Test Connection** to test the connection to your LDAP server.
 2. Once the LDAP server is successfully connected to MH-2300, users will be listed on the **LDAP User Name** table.

Step 4. Go to **Policy Object > Authentication > Group** and then set as shown below:



The Group Setting for User Authentication

Step 5. Go to **Policy > Outgoing** and then set as shown below:

- Select the authentication group for **Authentication**.
- Click **OK** to complete the settings.

Comment:

Add Policy

Source Address :	Inside Any ▼
Destination Address :	Outside Any ▼
Service :	Any ▼
Schedule :	----- None ----- ▼
Authentication :	LDAP_Auth ▼
VPN Trunk :	----- None ----- ▼

☒ Permit all outgoing connections ☐ Deny all outgoing connections

Action : Permit the selected:

☐ Port 1 (LAN1) ☐ Port 2 (LAN2) ☐ Port 3 (Port3) ☐ Port 4 (WAN2)
☐ Port 5 (WAN1)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼

Application Blocking : ----- None ----- ▼

☐ Advanced Settings

Creating a Policy to Apply the Authentication Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✓	🔒	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1 ▼

Policy Successfully Created

Step 6. The group members will be prompted for their authentication credentials to access the Internet. Click **Login** to complete the authentication procedure.

User Authentication - Login

Username :

Password :

The Authentication Prompt Screen

4.6 Application Blocking

This chapter will cover the configuration of *Application Blocking*, which allows for blocking the use of instant messaging, peer-to-peer file sharing, multimedia streaming, web-based email messaging, online gaming, VPN tunneling and remote controlling applications, as well as customizing their signatures.

Terms in Application Blocking

Application Signatures Settings

- The application signatures can be manually or automatically updated (on an hourly basis). Each update will display the time of update and the version number of signatures.

Instant Messenger Login

- Tick the boxes of messengers to be blocked. The options currently available are MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, Rediff, Web IM, AliSoft, BaiduHi, SinaUC, Fetion, Facebook Chat, Camfrog, LINE, WhatsApp, and Viber.

File Transfer over IM

- Tick the boxes of messengers to be blocked for file transfer. The options currently available are MSN, Yahoo, ICQ/AIM, QQ, Google Talk, and Gadu-Gadu.

Peer-to-Peer Sharing

- Tick the boxes of peer-to-peer file sharing applications to be blocked. The options currently available are eDonkey / eMule, BitTorrent / BitConnect, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, DirectConnect, iMesh, MUTE, Thunder5, GoGoBox, QQDownload, Ares, Shareaza, BearShare, Morpheus, Limewire, Kazaa, and FlashGet.

Multimedia Streaming

- Tick the boxes of multimedia streaming applications to be blocked. The options currently available are PPLive, PPStream, UUSee, QQLive, ezPeer, QVOD / BOBOHU, Funshion, PPMate, PiPi, StormCodec, SopCast, CNTV, and Xunlei Kan-Kan.

Web-Based Mail

- Tick the boxes of Web-based mail service providers to be blocked. The options currently available are Gmail, Hotmail, Yahoo, HiNet, PChome, URL, Yam, Seednet, 163/126/Yeah, Tom, Sina Ren-Ni-You, Sohu, and QQ Foxmail.

Online Gaming

- Tick the boxes of online games to be blocked. The options currently available are GLWorld, QQGame, and Xunlei Games.

VPN Tunneling

- Tick the boxes of VPN tunneling applications to be blocked. The options currently available are VNN Client, UltraSurf, Tor, Hamachi, Hotspot Shield, and FreeGate.

Remote Controlling

- Tick the boxes of remote controlling applications to be blocked. The options currently available are TeamViewer, VNC, Remote Desktop Connection, and ShowMyPC.

Other Applications

- Tick the boxes of other applications to be blocked. The options currently available are 10jqka, Dzh, Qianlong, HTTP Proxy, Socks4/5, DeskStock, Bump, Dropbox, and SkyDrive.

Terms in Custom

Name

- The name of the custom application signature.

Content Pattern

- To define the pattern of an application through matching the packet header, you may refer to the followings:
 - ◆ Type “google” to match the keyword of “google”.
 - ◆ Type “mail.google” to match the pattern prefix of “mail.google”.
 - ◆ Type “google.com\$” to match the pattern postfix of “google.com”.
 - ◆ Type “^mail.google.com\$” to match the exact pattern of “mail.google.com”

4.6.1 Examples of Blocking

4.6.1.1 Blocking the Use of IM Applications (including Messaging and File Transfer)

Step 1. Go to **Policy Object > Application Blocking > Settings** and then set as shown below:

- Specify a name in the **Rule Name** field.
- Tick the boxes of the **Select All** next to the **Instant Messenger Login** and **File Transfer over IM**.
- Click **OK**.

Add Application Blocking Rule

Rule Name : (Max. 20 characters)

Instant Messenger Login (<input checked="" type="checkbox"/> Select All)			
<input checked="" type="checkbox"/> MSN	<input checked="" type="checkbox"/> Yahoo	<input checked="" type="checkbox"/> ICQ/AIM	<input checked="" type="checkbox"/> QQ
<input checked="" type="checkbox"/> Skype	<input checked="" type="checkbox"/> Google Talk	<input checked="" type="checkbox"/> Gadu-Gadu	<input checked="" type="checkbox"/> Rediff
<input checked="" type="checkbox"/> WebIM	<input checked="" type="checkbox"/> AliSoft	<input checked="" type="checkbox"/> BaiduHi	<input checked="" type="checkbox"/> SinaUC
<input checked="" type="checkbox"/> Fetion	<input checked="" type="checkbox"/> Facebook Chat	<input checked="" type="checkbox"/> Camfrog	<input checked="" type="checkbox"/> LINE
<input checked="" type="checkbox"/> WhatsApp	<input checked="" type="checkbox"/> Viber		
File Transfer over IM (<input type="checkbox"/> Select All)			
<input type="checkbox"/> MSN	<input type="checkbox"/> Yahoo	<input type="checkbox"/> ICQ/AIM	<input type="checkbox"/> QQ
<input type="checkbox"/> Google Talk	<input type="checkbox"/> Gadu-Gadu		
Peer-to-Peer Sharing (<input type="checkbox"/> Select All)			
<input type="checkbox"/> Edonkey/eMule	<input type="checkbox"/> Bit Torrent/BitConnect	<input type="checkbox"/> WinMX	<input type="checkbox"/> Foxy
<input type="checkbox"/> KuGoo	<input type="checkbox"/> AppleJuice	<input type="checkbox"/> AudioGalaxy	<input type="checkbox"/> DirectConnect
<input type="checkbox"/> iMesh	<input type="checkbox"/> MUTE	<input type="checkbox"/> Thunder5	<input type="checkbox"/> GoGoBox
<input type="checkbox"/> QQDownload	<input type="checkbox"/> Ares	<input type="checkbox"/> Shareaza	<input type="checkbox"/> BearShare
<input type="checkbox"/> Morpheus	<input type="checkbox"/> Limewire	<input type="checkbox"/> KaZaa	<input type="checkbox"/> FlashGet
Multimedia Streaming (<input type="checkbox"/> Select All)			
<input type="checkbox"/> PPLive	<input type="checkbox"/> PPStream	<input type="checkbox"/> UUSEE	<input type="checkbox"/> QQLive
<input type="checkbox"/> ezPeer	<input type="checkbox"/> QvodPlayer/BoBoHu	<input type="checkbox"/> Funshion	<input type="checkbox"/> PPMate
<input type="checkbox"/> PiPi	<input type="checkbox"/> StormCodec	<input type="checkbox"/> SopCast	<input type="checkbox"/> CNTV
<input type="checkbox"/> Kankan	<input type="checkbox"/> KKBOX	<input type="checkbox"/> YouTube	<input type="checkbox"/> Youku
Web-Based Mail (<input type="checkbox"/> Select All)			
<input type="checkbox"/> Gmail	<input type="checkbox"/> Hotmail	<input type="checkbox"/> Yahoo	<input type="checkbox"/> Hinet
<input type="checkbox"/> PChome	<input type="checkbox"/> URL	<input type="checkbox"/> Yam	<input type="checkbox"/> Seednet
<input type="checkbox"/> 163/126/Yeah	<input type="checkbox"/> Tom	<input type="checkbox"/> Sina	<input type="checkbox"/> Sohu
<input type="checkbox"/> QQ			
Online Gaming (<input type="checkbox"/> Select All)			
<input type="checkbox"/> GLWorld	<input type="checkbox"/> QQGame	<input type="checkbox"/> XL Game	

Adding an IM Blocking Rule

Application Signatures Settings

Last updated on : 2014/12/15 10:01:03 (Signatures updated hourly)

Current version : 8.0.9 (Updated at 2014/11/27 08:00:22)

Manually update signatures (Using TCP port: 80 and UDP port: 53) [Update Now](#) [Test Connection](#)

Application Blocking Rules

1 / 1 Go		
Rule Name ▲	Application	Configuration
IM_Blocking	MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, ...	Modify Remove
1 / 1 Go		

[New Entry](#)

IM Blocking Rule Successfully Added

Step 1. Under **Policy > Outgoing**, set as shown below:

- **Application Blocking:** Select the IM blocking rule.
- Click **OK**.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (WAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled




Web Filter :

Application Blocking :

Advanced Settings

[OK](#) [Cancel](#)

Creating a Policy to Apply the IM Blocking Settings

<div>1 / 1</div> <div>Go</div>															
Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any										<div>Modify</div>	<div>Remove</div>	<div>Pause</div>	1 
<div>1 / 1</div> <div>Go</div>															

[New Entry](#)

Policy Successfully Created

4.6.1.2 Blocking the Use of P2P Applications (including File Download and Upload)

Step 1. Under **Policy Object > Application Blocking > Settings**, set as shown below:

- Specify a name for the rule.
- Tick the box of the **Select All** next to the **Peer-to-Peer Sharing**.
- Click **OK**.

Add Application Blocking Rule

Rule Name : (Max. 20 characters)

☐ Instant Messenger Login (☒ Select All)

☒ MSN

☒ Skype

☒ WebIM

☒ Fetion

☒ WhatsApp

☐ File Transfer over IM

☐ Peer-to-Peer Sharing

☐ Multimedia Streaming

☐ Web-Based Mail

☐ Online Gaming

☐ VPN Tunneling

☐ Remote Controlling

☐ Other Application

☐ Custom Application

☒ Yahoo

☒ Google Talk

☒ AliSoft

☒ Facebook Chat

☒ Viber

☒ ICQ/AIM

☒ Gadu-Gadu

☒ BaiduHi

☒ Camfrog

☒ QQ

☒ Rediff

☒ SinaUC

☒ LINE

Adding a P2P Blocking Rule

Application Signatures Settings

Last updated on : 2010/12/15 19:00:02 (Signatures updated hourly)

Current version : 6.3.2 (Updated at 2010/12/15 17:00:08)

Manually update signatures (Using TCP port: 80 and UDP port: 53) [Test Connection](#)

Application Blocking Rules

Rule Name ▲	Application	Configuration
P2P Blocking	Edonkey/eMule, Bit Torrent/BitConnect, WinMX, Foxy, KuGoo, AppleJui...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

P2P Blocking Rule Successfully Added

Step 2. Under **Policy > Outgoing**, set as shown below:

- **Application Blocking:** Select the rule.
- Click **OK**.

Add Policy

Source Address : Inside Any

Destination Address : Outside Any

Service : Any

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (WAN2) ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : P2P Blocking

Advanced Settings

OK
Cancel

Creating a Policy to Apply the P2P Blocking Settings

Policy Successfully Created

Note

P2P applications are the major cause of bandwidth exhaust and also are hard to block its use due to the port alternation. Accordingly, **Application Blocking** provides a more effective way to block the use of P2P applications by its packet signatures rather than port number.

4.7 Virtual Server

This chapter will cover the configuration of *Virtual Server*, which allows for providing services to the public by mapping public IP addresses to private IP addresses.

- **Mapped IPs:** Maps a public IP address to a private IP address by using Network Address Translation (NAT) to provide multiple services.
- **Port Mapping:** Maps a public IP address to multiple private IP addresses by using Port Address Translation (PAT) to provide multiple services or a

single service via load balancing algorithm.

- **Port-Mapping Group:** Group feature is available for **Mapped IPs** and **Port Mapping** settings to simplify the process of applying addresses to network policies.

Terms in Mapped IPs

Mapped IP Address

- Specify the IP address of a WAN port to be mapped.

Host IP Address

- Specify an IP address for the internal host.

Terms in Port Mapping

Public IP Address

- Specify an IP address for the virtual server.

Service

- Select a service from the drop-down list.

External Service Port

- Specify a port number for the service. The service port allows modification if there is only one port being used for providing the service. For example, the default port for accessing the HTTP websites is "80", it may be changed into any other valid port. Yet, HTTP access requires new port to be appended to the website address, such as `http://www.yahoo.com:8080`.

Load Balancing

- **Round-Robin:** In this mode, sessions are allocated to the internal servers by means of a round-robin cycle. This improves overall efficiency and prevents the entire load being placed on just a single server.
- **Redundancy:** When the main server ceases to function, the sessions will then be allocated to the backup servers according to their number on the list.
- **Source IP Hash:** Sessions are allocated according to the source IP.

Interface

- Select the subnet that the virtual server is located in.

Private IP Address

- Specify an IP address for the virtual server.

4.7.1 Examples of Virtual Server

Prerequisite Configuration (Note: IP addresses are used as example only)

Apply for two ADSL lines with static IP addresses from a local ISP.

Configure Port1 as LAN1 (192.168.1.1, NAT/ Routing Mode) and connect to the LAN subnet 192.168.1.x / 24

Configure Port2 as WAN1 with the ISP-allocated IP addresses 61.11.11.10 to 61.11.11.14.

Configure Port3 as WAN2 with the ISP-allocated IP addresses 211.22.22.18 to 211.22.22.30.

4.7.1.1 Using a Policy-managed Server to Provide Multiple Services (FTP, Web, Mail, etc.)

Step 1. Run a server on 192.168.1.100 and resolve the domain name using an external server to provide FTP, Web, and mail services.

Step 2. Under **Policy Object > Address > LAN**, set as shown below:

Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 1 MB)

[Assist Me](#)

Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		In Use
Main_Server	IPv4	All	192.168.1.100 / 255.255.255.255		Modify Remove

[New Entry](#)

The Address Setting for the Server IP Address

Step 3. Under **Policy Object > Virtual Server > Mapped IPs**, set as shown below:

- Click **New Entry**.
- Specify a name for the mapped IP address setting.
- **Mapped IP Address**: Select "Port 2 (WAN 1)" from the corresponding drop-down list and then specify 61.11.11.12 in the field or click [Assist Me](#) to select an address.
- **Host IP Address** : Select "Port 1 (LAN 1)" from the corresponding drop-down list and then specify 192.168.1.100 in the field or click [Assist Me](#) to select an address.
- Click **OK**.

Add Mapped IP Address [Help](#)

Name : (Max. 20 characters)

Mapped IP Address : Port2 (WAN1) [Assist Me](#)

Host IP Address : Port1 (LAN1) [Assist Me](#)

[OK](#) [Cancel](#)

Creating a Mapped IP Address

Step 4. Under **Policy Object > Service > Group** add a group named “Main_Service” which is consisted of DNS, FTP, HTTP, POP3, and SMTP services. Next, add another one named “Mail_Service” to group DNS, POP3, and SMTP services.

Group Name ▲	Group Items	Configuration	
Main_Service	DNS, HTTP, POP3, SMTP	Modify	Remove
Mail_Service	DNS, POP3, SMTP	Modify	Remove

New Entry

The Group Settings for Server IP Addresses

Step 5. Under **Policy > Incoming**, set as shown below:

- Select the mapped IP (61.11.11.12) for **Destination Address**.
- Select “Mail_Service” for **Service**.
- Click **OK**.

Add Policy

Source Address :
Destination Address :
Service :
Schedule :
Authentication :
VPN Trunk :

☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :
Packet Logging :
Traffic Grapher :

Advanced Settings

OK Cancel

Creating a Policy to Apply the Service Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Mapped IP](61.11.11.12)	Main_Servi...	✓		Modify Remove Pause	1

New Entry

Policy Successfully Created

Step 6. Under **Policy > Outgoing**, set as shown below:

- **Source Address:** Select the LAN address group of the servers.
- **Service:** Select "Mail_Service".
- Click **OK**.

Add Policy

Source Address : Main_Server

Destination Address : Outside Any

Service : Mail_Service

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☒ Permit All
 ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
☐ Permit Port 2 (WAN1)
☐ Permit Port 3 (WAN2)
☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

OK
Cancel

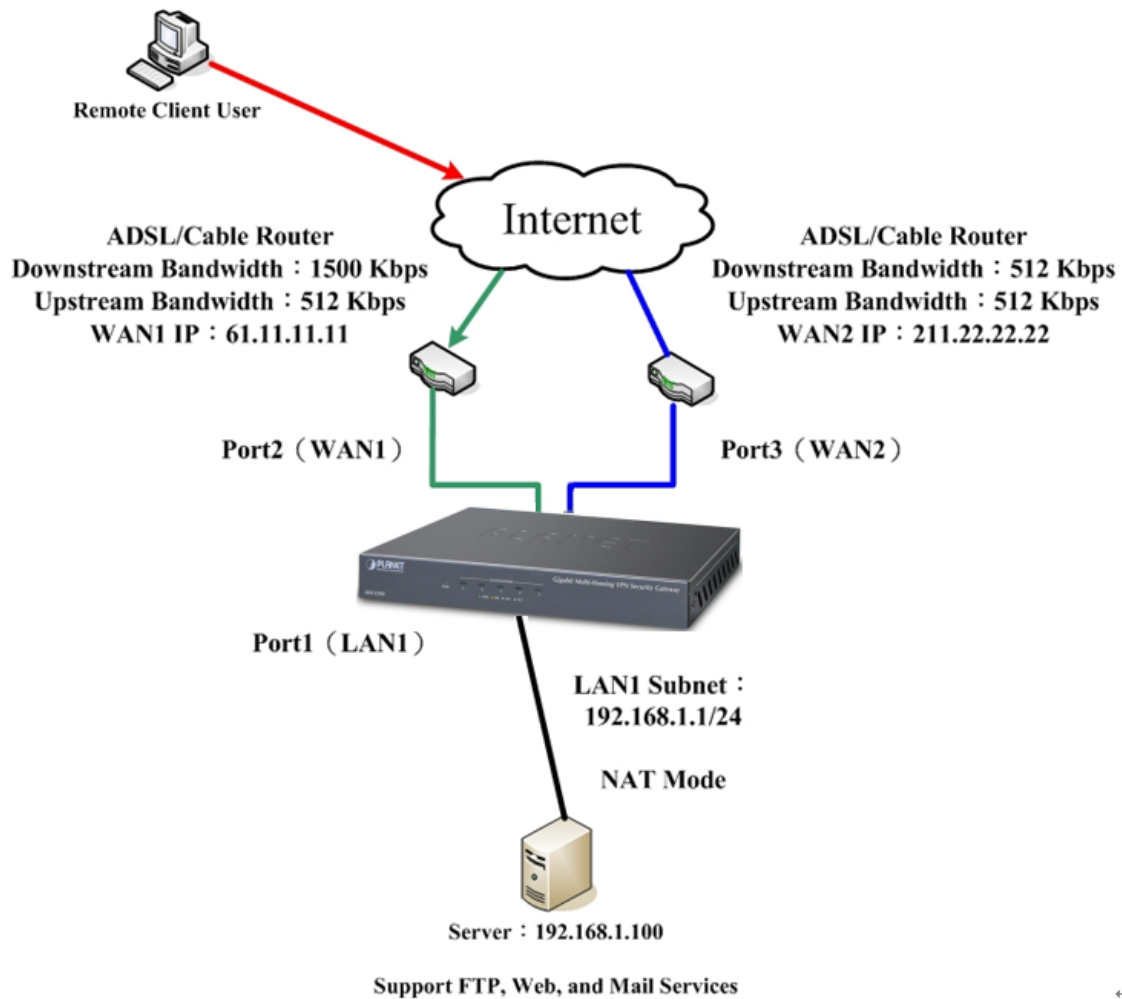
Creating a Policy to Apply the Service Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Main_Server	Outside Any	Mail_Service	✓		Modify Remove Pause	1


New Entry

Policy Successfully Created

Step 7. Services are open to the public through the mapped IP address.



The Deployment of a Server Providing Multiple Services through Address Mapping


Note

For the sake of security, it is not suggested selecting “Any” for **Service** when applying a mapped IP to a policy. It may expose your network vulnerabilities to cyber attacks.

4.7.1.2 Using Multiple Policy-managed Servers to Host a Website

- Step 1. Run multiple Web servers separately on 192.168.1.101, 192.168.1.102, 192.168.1.103 and 192.168.1.104.
- Step 2. Under **Policy Object > Virtual Server > Port Mapping**, set as shown below:
- Specify a name for the port mapping setting.
 - **Public IP Address:** Select “Port3 (WAN2)” from the corresponding drop-down list and then specify 211.22.22.23 in the field or click [Assist Me](#) to select an address.
 - **Service:** Select “HTTP(80)”.
 - **External Service Port:** Modify from “80” to “8080”.

- **Load Balancing:** Select "Round-Robin".
- **Interface:** Select "LAN".
- **Private IP Address # 1:** Specify "192.168.1.101" in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.
- **Private IP Address # 2:** Specify "192.168.1.102" in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.
- **Private IP Address # 3:** Specify "192.168.1.103" in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.
- **Private IP Address # 4:** Specify "192.168.1.104" in the field or click [Assist Me](#) to select an address.
- Click **OK**.

Add Port Mapping Help

Name : (Max. 20 characters)

Public IP Address : Port2 (WAN1) Assist Me

Service :

External Service Port :

Load Balancing :

Interface : Assist Me

Private IP Address # 1 :

Private IP Address # 2 :

Private IP Address # 3 :

Private IP Address # 4 :

Creating a Port Mapping Rule

Name ▲	Public IP Address	Service	Private IP Address #	Configuration
HTTP Server	211.74.99.122 Port2 (WAN1)	HTTP	192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 (LAN)	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The Mapping Rule for the HTTP Service

Step 3. Under **Policy > Incoming**, set as shown below:

- **Destination IP:** Select the mapped IP (211.22.22.23).
- **Service:** Select "HTTP(8080)".
- Click **OK**.

Add Policy

Source Address :	Outside Any
Destination Address :	[Port Mapping] HTTP Server(211.74.99.122)
Service :	HTTP (8080)
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	----- None -----

☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :
 Packet Logging : ☐ Enabled
 Traffic Grapher : ☐ Enabled

☐ Advanced Settings


Creating a Policy for the HTTP Service



Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](211.74.9...	HTTP	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

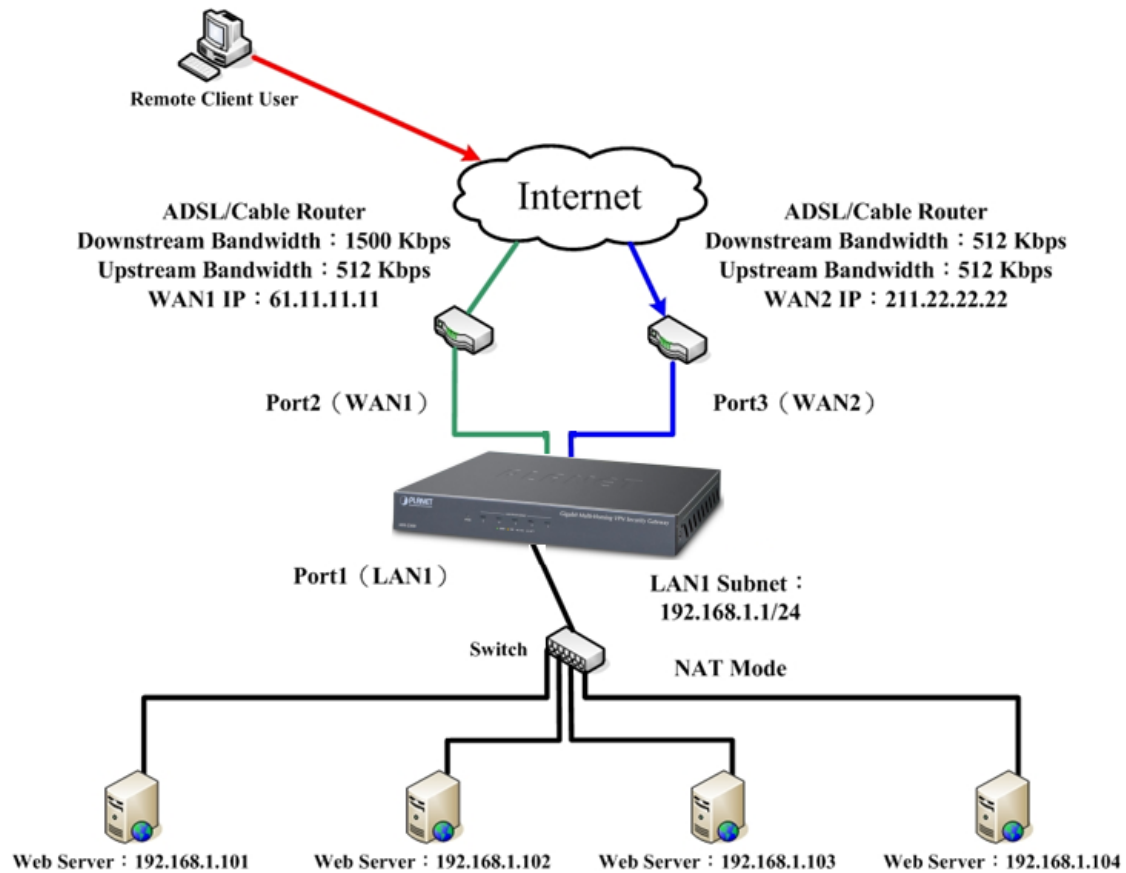


Policy Successfully Created


Note

External Web server requests will require appending the new port to the website address, such as <http://www.yahoo.com:8080>.

Step 4. Web servers are available for public access through the port mapping setting.



The Deployment of Multiple Servers Hosting a Website through Port Mapping

4.7.1.3 Permitting VoIP Telephony between External and Internal Users via TCP 1720, TCP 15323-15333 and UDP 15323-15333

Step 1. Assign the address 192.168.1.100 to the VoIP service.

Step 2. Under **Policy Object > Address > LAN**, set as shown below:

Export data entries :

Import data entries : (Max. file size: 1 MB)

[Assist Me](#)

Name	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		<input type="button" value="In Use"/>
VoIP	IPv4	All	192.168.1.100 / 255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The Address Setting for VoIP Communication

Step 3. Add a service setting under **Policy Object > Service > Custom** as follows:

Name ▲	Protocol Type	Client Port	Server Port	Configuration
VoIP	TCP	0 - 65535	1720 - 1720	Modify Remove

[New Entry](#)

The Service Setting for VoIP Communication

Step 4. Under **Policy Object > Virtual Server > Port Mapping**, set as shown below:

- **Name** : Specify a name for the port mapping setting.
- **Public IP Address**: Select "Port 2 (WAN1)" from the corresponding drop-down list and then specify "61.11.11.12" in the field, or click [Assist Me](#) to select an address.
- **Service**: Select the custom service.
- **External Service Port** is defaulted.
- **Load Balancing**: Select "Round-Robin".
- **Interface**: Select "LAN".
- **Private IP Address # 1**: Specify "192.168.1.100" in the field or click [Assist Me](#) to select an address.
- Click **OK**.

[Help](#)

Name : (Max. 20 characters)

Public IP Address : Port2 (WAN1) ▼ [Assist Me](#)

Service : [Custom Service] VoIP ▼

External Service Port : Custom Service

Load Balancing : Round-Robin ▼

Interface : LAN ▼ [Assist Me](#)

Private IP Address # 1 : [Next Row](#)

[OK](#)

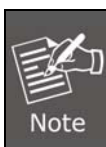
[Cancel](#)

Creating a Port Mapping Rule

Name ▲	Public IP Address	Service	Private IP Address #	Configuration
VoIP	61.11.11.12 Port2 (WAN1)	VoIP	192.168.1.100 (LAN)	Modify Remove

[New Entry](#)

The Mapping Rule for the VoIP Service



The External Service Port allows modification if there is only one port being used for providing the service.

Step 5. Under **Policy > Incoming**, set as shown below:

- **Destination IP:** Select the mapped IP (61.11.11.12).
- **Service:** Select the custom service.
- Click **OK**.

Add Policy

Source Address :

Outside Any

Destination Address :

[Port Mapping] VoIP(61.11.11.12)

Service :

VoIP

Schedule :

----- None -----

Authentication :

----- None -----

VPN Trunk :

----- None -----

☒ Permit connections from Incoming

☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging :
☐ Enabled

Traffic Grapher :
☐ Enabled

⚙️
Advanced Settings

OK

Cancel

Creating a Policy for Allowing Incoming VoIP Traffic

⏮ ⏪ ⏩ ⏭ / 1 ⏪ ⏭ ⏮

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](61.11.11....	VoIP	✔		<div style="display: flex; justify-content: space-around; font-size: 0.8em;"> Modify Remove Pause </div>	1

⏮ ⏪ ⏩ ⏭ / 1 ⏪ ⏭ ⏮

New Entry

Policy Successfully Created

Step 6. Under **Policy > Outgoing**, set as shown below:

- **Source Address:** Select the IP address assigned for VoIP service.
- **Service:** Select the VoIP service.
- **Action:** Select "Port2 (WAN1)".
- Click **OK**.

Add Policy

Source Address : VoIP

Destination Address : Outside Any

Service : VoIP

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☐ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
 ☒ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

Creating a Policy for Allowing Outgoing VoIP Traffic

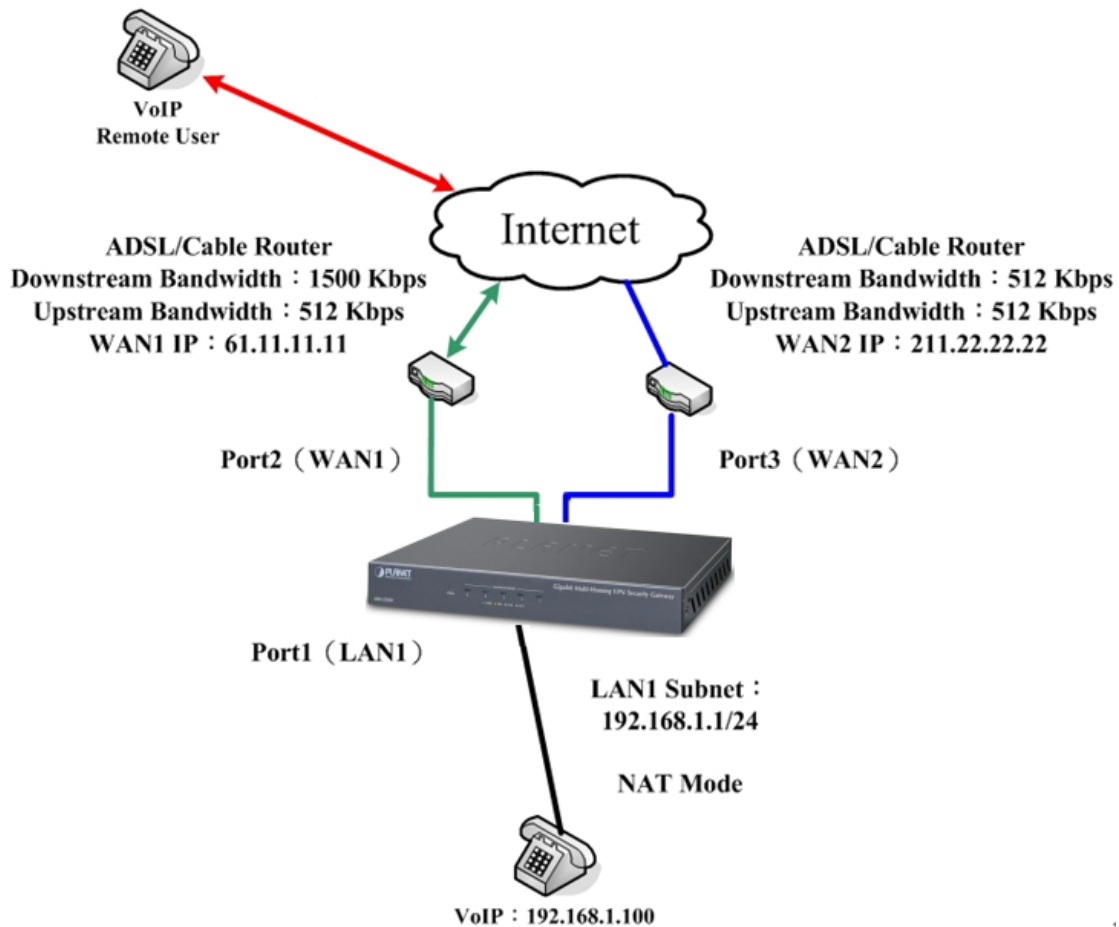
OK Cancel

Source	Destination	Service	Action	Options	Co	Priority
VoIP	Outside Any	VoIP	1		<div style="display: flex; justify-content: space-between; align-items: center;"> Modify Remove Pause </div>	1

Total entries : 1

Policy Successfully Created

Step 7. VoIP communication is available between external and internal users through the port mapping setting.



The Deployment of VoIP Communication through Port Mapping

4.7.1.4 Using Multiple Policy-managed Servers to Provide HTTP, POP3, SMTP, and DNS Services

Step 1. Run multiple servers separately on 192.168.1.101, 192.168.1.102, 192.168.1.103, and 192.168.1.104, and resolve the domain name using an external server to provide multiple services.

Step 2. Under **Policy Object > Address > LAN / LAN Group**, set as shown below:

Export data entries : [Export](#)

Import data entries : [Browse](#) [Import](#) (Max. file size: 1 MB)

[Assist Me](#)

Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
Inside Any	---	All	---		In Use
Server1	IPv4	All	192.168.1.101 / 255.255.255.255		Modify Remove
Server2	IPv4	All	192.168.1.102 / 255.255.255.255		Modify Remove
Server3	IPv4	All	192.168.1.103 / 255.255.255.255		Modify Remove
Server4	IPv4	All	192.168.1.104 / 255.255.255.255		Modify Remove

[New Entry](#)

The Address Settings for the Servers

Name ▲	Group Members	Configuration
Server Group	Server1, Server2, Server3, Server4	Modify Remove

[New Entry](#)

The Group Setting for Server IP Addresses

Step 3. Under **Policy Object > Service > Group**, add a group named “Main_Service” which is consisted of DNS, HTTP, POP3, and SMTP services. Next, add another one named “Mail_Service” to group DNS, POP3, and SMTP services.

Group Name ▲	Group Items	Configuration
Main_Service	DNS, HTTP, POP3, SMTP	Modify Remove
Mail_Service	DNS, POP3, SMTP	Modify Remove

[New Entry](#)

Service Group Settings

Step 4. Under **Policy Object > Virtual Server > Port Mapping**, set as shown below:

- Name: Specify a name for the port mapping setting.
- **Public IP Address**: Select “Port 3 (WAN 2)” from the corresponding drop-down list and then specify 211.22.22.23 in the field or click [Assist Me](#) to select an address.
- Select the pre-defined service for **Service**.
- **External Service Port** is defaulted..
- **Load Balancing**: Select “Round-Robin”.
- **Interface**: Select “LAN”.
- Private IP Address # 1: Specify “192.168.1.101” in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.

- Private IP Address # 2: Specify "192.168.1.102" in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.
- Private IP Address # 3: Specify "192.168.1.103" in the field or click [Assist Me](#) to select an address. Click **Next Row** when done.
- Private IP Address # 4: Specify "192.168.1.104" in the field or click [Assist Me](#) to select an address.
- Click **OK**.

Modify Port Mapping

[Help](#)

Name : (Max. 20 characters)

Public IP Address : Port2 (WAN1) [Assist Me](#)

Service :

External Service Port : Group Service

Load Balancing :

Interface : [Assist Me](#)

Private IP Address # 1 :

Private IP Address # 2 :

Private IP Address # 3 :

Private IP Address # 4 :

Creating a Port Mapping Entry

Name ▲	Public IP Address	Service	Private IP Address #	Configuration
Server Group	211.22.22.23 Port2 (WAN1)	Main_Service	192.168.1.101 192.168.1.102 192.168.1.103 192.168.1.104 (LAN)	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

The Mapping Rule for the Servers

Step 5. Go to **Policy > Incoming** and then set as shown below:

- Select the mapped IP (211.22.22.23) for **Destination Address**.
- Select “Main_Service” for **Service**.
- Click **OK**.

Add Policy

Source Address : Outside Any ▼

Destination Address : [Port Mapping] Server Group(211.22.22.23) ▼

Service : Main_Service ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : ----- None ----- ▼

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Advanced Settings

Creating a Policy to Apply the Service Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](211.22.2...	Main_Servi...	✓		<div style="display: flex; justify-content: space-around; padding: 2px;"> Modify Remove Pause </div>	1 ▼

Policy Successfully Created

Step 6. Go to **Policy > Outgoing** and set as shown below:

- Select the LAN address group of the servers for **Source Address**.
- Select "Mail_Service" for **Service**.
- Click **OK**.

Add Policy

Source Address : Server Group

Destination Address : Outside Any

Service : Main_Service

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : ----- None -----

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (Port4)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

OK
Cancel

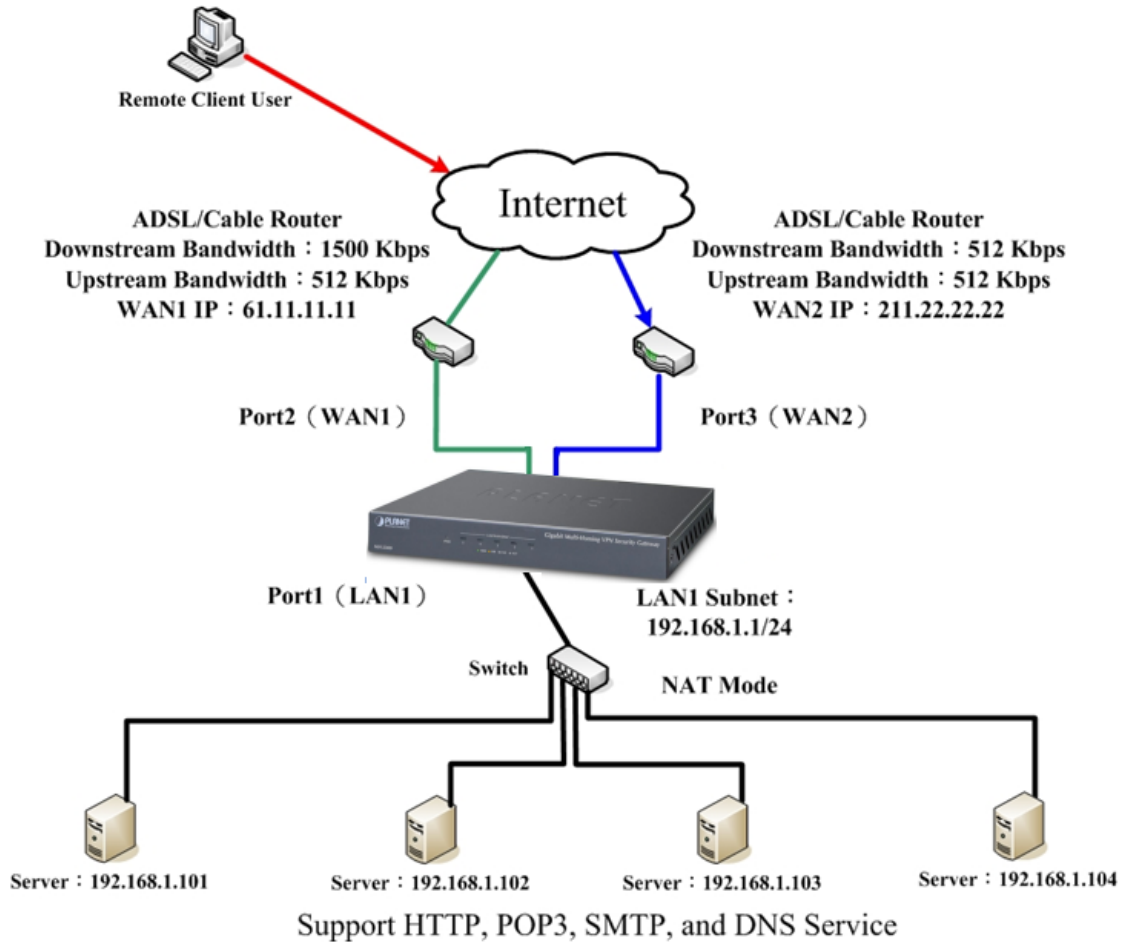
Creating a Policy to Apply the Service Group Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Server Group	Outside Any	Main_Servi...	✓		Modify Remove Pause	1

New Entry

Policy Successfully Created

Step 7. Services are open to the public through the port mapping setting.



The Deployment of Multiple Servers Providing Services through Port Mapping

4.8 VPN

This chapter will cover the configuration of *VPN*, which allows for establishing private and secure site-to-site connections, enabling network to be built among distributed locations and in a convenient way.



Note

To set up a secure and encrypted VPN network, it requires applying the **IPSec Autokey / PPTP Server / PPTP Client** settings to a **Trunk** setting under **Policy Object > VPN** and then to a network policy.

Terms in VPN

Diffie-Hellman

- A cryptographic protocol that allows two parties that have no prior knowledge of each other to establish a shared secret key over an insecure communication channel.

RSA

- An asymmetric cryptography that involves a public and private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

Pre-Shared Key String

- A string of Unicode characters that is used to authenticate Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPSec) connections.

ISAKMP (Internet Security Association and Key Management Protocol)

- A protocol that is used to establish **Security Associations (SA)** and cryptographic keys in an Internet environment. **ISAKMP** provides a framework for authentication and key exchange. It is designed to be key exchange independent. Authenticated keying material for use with ISAKMP are provided by protocols such as Internet Key Exchange and Kerberized Internet Negotiation of Keys.

Main Mode

- When associating IKE certificates, the device offers main mode and aggressive mode to choose from. The main mode requests sending 6 messages mutually before starting the data exchange, it is to confirm the identity of both parties, ensuring the data transferring security.

Aggressive Mode

- The aggressive mode requests sending 3 messages mutually before starting the data exchange, it is to confirm the identity of both parties, ensuring the data transferring security.

AH (Authentication Header)

- The Authentication Header guarantees connectionless integrity and data origin authentication of IP datagrams.

ESP (Encapsulating Security Payload)

- The Encapsulated Security Payload provides confidentiality and integrity protection to IP datagrams.

DES (Data Encryption Standard)

- The Data Encryption Standard is a NIST standard encryption using 56-bit key.

3DES (Triple-DES)

- Triple DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times. It can achieve an algorithm up to 168 bits.

AES (Advanced Encryption Standard)

- The Advanced Encryption Standard (AES) is a symmetric key encryption technique, usually using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.

NULL Algorithm

- The NULL Algorithm is an instant and convenient alternative for connection. It is merely a simple replacement for ESP (Encapsulating Security Payload) without any cryptograph protection.

SHA1 (Secure Hash Algorithm-1)

- The SHA1 is a revision of SHA (Secure Hash Algorithm). It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.

MD5 Algorithm

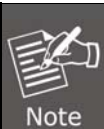
- MD5 (Message Digest Algorithm 5) processes a variable-length message into a fixed-length output of 128 bits.

GRE / IPSec

- The GRE (Generic Routing Encapsulation) comes in packet packing function without any encryption against monitoring and attacking. Normally, the GRE needs to cooperate with IPSec so as to provide a secure connection.

Extended Authentication (XAuth)

- XAuth provides an additional level of authentication. It uses a Request/Reply mechanism to provide the extended authentication. XAuth is also referred to as two factor authentication.



The **Account Name** under **Extended Authentication (XAuth)** are the accounts listed under **Policy > Authentication > Account**.

Terms in One-Step IPSec

One-Step IPSec

- IPSec VPN can be established within just one step as follows:
 - ◆ Go to **Policy Object > VPN > One-Step IPSec** and then refer to the following:
 - Specify a name for the IPSec rule.
 - Select a WAN port for **Interface**.
 - Tick the radio box of "LAN 1" (leave the drop-down list as default).
 - Specify the **Remote Gateway (Static IP or Hostname)**.
 - Specify the **Remote IP Address / Netmask**.
 - Type a string as the pre-shared key.
 - Click **OK** to complete the settings.

- The corresponding autokey, trunk and policy settings will be automatically added.

Help

Name : (Max. 20 characters)

Local Settings:
 Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2)
 Local IP Address / Netmask : ☒ LAN1

Remote Settings:
 Remote Gateway (Static IP or Hostname) :
 Remote IP Address / Netmask : /
 Pre-Shared Key String :

OK
Cancel

Adding a One-Step IPsec Rule

1 / 1 Go

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	ipsec	WAN1	211.22.22.22	DES / MD5	---	<div style="border: 1px solid #ccc; padding: 2px 5px; color: green;">Modify</div>

1 / 1 Go

New Entry

One-Step IPsec Rule Successfully Added

1 / 1 Go

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec_T	192.168.1.1 / 24	192.168.2.0 / 24	ipsec	<div style="border: 1px solid #ccc; padding: 2px 5px; color: green;">Modify</div>

1 / 1 Go

New Entry

A VPN Trunk Created Correspondingly

1 / 1 Go

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		<div style="border: 1px solid #ccc; padding: 2px 5px; color: green;">Modify</div> <div style="border: 1px solid #ccc; padding: 2px 5px; color: orange;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 5px; color: gray;">Pause</div>	1 ▼

1 / 1 Go

New Entry

An Outgoing Policy Created Correspondingly


1 / 1 Go

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<div style="border: 1px solid #ccc; padding: 2px 5px; color: green;">Modify</div> <div style="border: 1px solid #ccc; padding: 2px 5px; color: orange;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 5px; color: gray;">Pause</div>	1 ▼

1 / 1 Go

New Entry

An Incoming Policy Created Correspondingly


 Note

For the convenience of quick VPN connection, **One-Step IPsec** uses default settings for some of the configurations as listed below:

- IKE Negotiation: Main mode
- Authentication Method: Pre-Shared Key
- ISAKMP Settings: DES + MD5 + Diffie-Hellman 1
- IPsec Settings: DES + MD5
- The corresponding autokey, trunk and policy settings will be automatically added.

Terms in VPN Wizard

VPN Wizard

- Follow the steps below to establish a VPN connection:
 - ◆ Under **Policy Object > VPN > VPN Wizard**, set as shown below:
 - Select a connection type and then click **Next**.
 - Create a policy object for the VPN connection. Click **Next** when done.
 - Apply the policy object to a VPN trunk. Click **Next** when done.
 - Select the VPN trunk.
 - Click **Finish**.
 - The corresponding incoming and outgoing policies will be automatically added for the VPN connection.

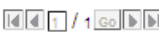
VPN Tunnel Wizard


☒ IPsec VPN
☐ PPTP VPN Server
☐ PPTP VPN Client

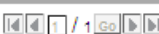
Next

Selecting a Connection Type

IPsec Tunnel Settings



Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	ipsec1	WAN1	61.62.236.15	DES / MD5	—	<div style="display: flex; justify-content: space-around;"> <div style="background-color: #4CAF50; color: white; padding: 2px 10px;">Modify</div> <div style="background-color: #FF9800; color: white; padding: 2px 10px;">Remove</div> </div>



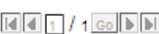
New Entry


Back

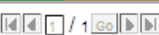
Next

Creating a VPN Policy Object

VPN Trunk Settings



Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.1.0 / 24	172.16.0.1 / 24	ipsec1	<div style="display: flex; justify-content: space-around;"> <div style="background-color: #4CAF50; color: white; padding: 2px 10px;">Modify</div> <div style="background-color: #FF9800; color: white; padding: 2px 10px;">Remove</div> </div>



New Entry

Back

Next

The VPN Policy Object Applied to a VPN Trunk

Default Policy Settings

Select All Invert All

=====Available Trunk=====

Add >>

<< Remove

Select All Invert All

=====Applied Trunk=====

ipsec-vpn-trunk

Back Finish

Applying the VPN Trunk to Network Policies

PLANET Networking & Communication

Policy Object > VPN > VPN Wizard

System

Network

Policy Object

Address

VPN wizard completed.

VPN Wizard Successfully Completed

[Navigation icons]

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1

[Navigation icons]

An Outgoing Policy Created Correspondingly

[Navigation icons]



Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1

[Navigation icons]

An Incoming Policy Created Correspondingly

Terms in IPSec Autokey

The description of the symbols used for connection status are as follows:

Symbol		
Description	Disconnected	Connected

Name

- The name of an IPSec rule. Note that the name cannot be repeated under **Policy Object > VPN > IPSec Autokey**.

Interface

- The external interface of your local gateway.

Gateway

- The external interface of the remote gateway.

Algorithm

- The encryption method employed by a VPN connection.

Uptime

- The elapsed time of an established VPN connection.

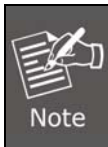
Configuration

- Click **Modify** or **Remove** to edit or delete the corresponding rule.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

[New Entry](#)

IPSec Autokey Rule Table





An IPSec VPN connection is maintained using **Peer Status Detection** mechanism and can be manually established when **Remote Gateway (Static IP or Hostname)** is specified within the IPSec autokey rule.

Terms in PPTP Server

PPTP Server

- Followed by an “Enabled” or “Disabled” to indicate the activation status of PPTP server.
- External RADIUS authentication is supported.
- Allows for assigning the IP addresses of PPTP client, DNS server, and WINS server.
- The description of the symbols used for connection status are as follows:

Symbol		
Description	Disconnected	Connected

Username

- The name of an authenticated PPTP client.

Client IP

- The assigned IP address of a PPTP client.

Uptime

- The elapsed time of an established VPN connection.

Configuration


- Click **Modify** or **Remove** to edit or delete the corresponding rule.

PPTP Server (Enabled) [Modify](#)

Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 20 KB)


1 / 1 [Go](#)

Status	Username	Client IP	Uptime	Configuration
	sukent	0.0.0.0	---	Modify Remove

1 / 1 [Go](#)

[New Entry](#)

The PPTP Server Rule Table





A PPTP VPN connection is maintained using **Echo-Request** mechanism and can be manually disconnected by ticking the box of "Manual disconnection" within the PPTP server rule.

Terms in PPTP Client

Status

- The description of the symbols used for connection status are as follows.

Symbol		
Description	Disconnected	Connected

Username

- The name of an authenticated PPTP client.

Server IP or Hostname

- The IP address or host name of a connected PPTP server.

Encryption

- The encryption status of an established VPN connection.

Uptime

- The elapsed time of an established VPN connection.


Configuration

- Click **Modify** or **Remove** to edit or delete the corresponding rule.

Status	Username	Server IP or Hostname	Encryption	Uptime	Configuration
No data found!					

[New Entry](#)

The PPTP Client Rule Table





A PPTP VPN connection is maintained using **Echo-Request** mechanism and can be manually connected by ticking the box of “Manual connection” within the PPTP client rule.

Terms in Trunk

Status

- The description of the symbols used for connection status are as follows.

Symbol		
Description	Disconnected	Connected

Name

- The name of a trunk rule. Note that the name cannot be repeated under **Policy Object > VPN > Trunk**.

Local Subnet

- The IP address of source subnet.

Remote Subnet

- The IP address of destination subnet.

Tunnel Selecton

- The IPSec or PPTP tunnels that are included in the trunk.


Configuration

- Click **Modify** or **Remove** to edit or delete the corresponding rule.

Status	Username ▲	Client IP	Uptime	Configuration
No data found !				

[New Entry](#)

The Trunk Rule Table



Once the **Trunk Load Balancing** is enabled, the VPN tunnels will be load-balanced to increase the link speed. (Note that this feature requires two units of the same model at both ends of a VPN connection to be activated, and is also subject to the **Load Balancing Mode** specified under **Network > Interface**.)

Terms in Trunk Group

Name

- The name of a trunk group. Note that the name cannot be repeated under **Policy Object > VPN > Trunk Group**.

Group Member

- The group of trunk rules that are to be applied to a policy.

Configuration

- Click **Modify** or **Remove** to edit or delete the corresponding rule.

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
No data found!					

[New Entry](#)

The Trunk Group Table

4.8.1 Examples of VPN

4.8.1.1 Using Two Units of MH-2300 to Establish an IPSec VPN Tunnel for Private Network Access

Prerequisite Configuration (Note: The IP addresses are used as examples only.)

Company A: Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Company B: Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x / 24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

Port 1 is added with a multiple subnet (192.168.85.1) and is connected to the LAN subnet 192.168.85.x / 24

This example will be using two units of MH-2300 to establish a VPN tunnel for private network access as follows:

For Company A, set as shown below:

Step 1. Go to **Policy Object > VPN > IPSec Autokey**, and then click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

[New Entry](#)

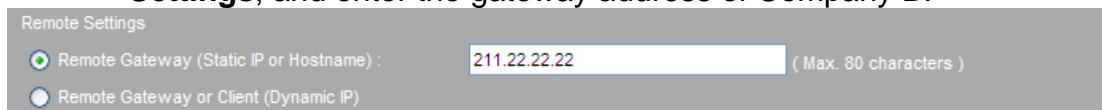
The IPSec Autokey Rule Table

Step 2. Enter "VPN_A" in the **Name** field and select "Port 2 (WAN 1)" for **Interface**

Basic Settings (Required)	
Name :	<input type="text" value="IPSec tunne"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

The Name and Interface Settings

Step 3. Select “Remote Gateway (Static IP or Hostname)” for **Remote Settings**, and enter the gateway address of Company B.



Remote Settings

☒ Remote Gateway (Static IP or Hostname) : 211.22.22.22 (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

The Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of the string is 62 characters.)



Authentication Method : Pre-Shared Key

Pre-Shared Key String : 1234567890 (Max. 62 characters)

The Authentication Method Settings

Step 5. In the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, select “MD5” for **Authentication Algorithm**, and select “Diffie-Hellman 1” for **Key Group**.



Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

Key Group : Diffie-Hellman 1

The Encryption and Data Integrity Algorithms

Step 6. Select the radio box of “Use both algorithms” under the **IPSec Settings** section, select “3DES” for **Encryption Algorithm**, and select “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

The IPSec Algorithm Settings

Step 7. In the **Advanced Settings (Optional)** section, select “DH 1” for **PFS Key Group**, enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field, and then select “Main Mode” for **IKE Negotiation**.



PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

The Advanced Settings

Step 8. The IPSec autokey rule is successfully added.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	IPSec_tunnel	WAN1	211.22.22.22	3DES / MD5	—	Modify Remove

1 / 1 Go

Total entries : 1

[New Entry](#)

IPSec Autokey Rule Successfully Added

Step 9. Under **Policy Object > VPN > Trunk**, set as shown below:

- Specify a name for the VPN trunk.
- **Local Settings** : Select “LAN” for **Interface** and specify the subnet and netmask of Company A.
- **Remote Settings**: Specify the subnet and netmask of Company B.
- **Tunnel Selection**: Select “VPN_A” from the **Available Tunnels** column on the left and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

Available Tunnels

Add >>

<< Remove

Applied Tunnels

IPSec_tunnel

Keepalive IP Address :


☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

[OK](#)

[Cancel](#)

Adding a VPN Trunk

Status	Name	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	IPSec_vpn-tunnel	192.168.10.0 / 24	192.168.85.0 / 24	IPSec_tunnel	Modify Remove

1 / 1 Go

[New Entry](#)

VPN Trunk Successfully Added

Step 10. Under **Policy > Outgoing**, set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

Application Blocking :

☐ Advanced Settings

[OK](#) [Cancel](#)

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1

1 / 1 Go

[New Entry](#)

Policy Successfully Created

- Step 11. Under **Policy > Incoming**, set as shown below:
- Select the VPN trunk for **VPN Trunk**.
 - Click **OK**.

Add Policy

Source Address :	Outside Any	▼
Destination Address :	Inside Any	▼
Service :	Any	▼
Schedule :	----- None -----	▼
Authentication :	----- None -----	▼
VPN Trunk :	IPSec_vpn-tunnel	▼

Action :

☒ Permit connections from Incoming

☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options					Configuration			Priority
Outside Any	Inside Any	Any	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	1 ▼

Policy Successfully Created

Note

If **Remote Settings** is selected for **Remote Gateway** or **Client (Dynamic IP)** under **Policy Object > VPN > IPSec Autokey**, then **Aggressive Mode** is compulsory for IKE Negotiation as well as **Local** and **Peer IDs** are required for the VPN connection.

For Company B, set as shown below:

- Step 1. Under **System > Configuration > Multiple Subnets**, set as shown below:

Name ▲	IP Version	Alias IP Address / Netmask	Interface	VLAN ID	Configuration	
subnet1	IPv4	192.168.85.1 / 255.255.255.0	LAN1		<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

Network Subnet Successfully Added

Step 2. Go to **Policy Object > VPN > IPSec Autokey** and then click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

[New Entry](#)

The IPSec Autokey Rule Table

Step 3. Enter “VPN_B” in the **Name** field and then select “Port2 (WAN1)” for **Interface**.

Basic Settings (Required)	
Name :	<input type="text" value="IPSec_tunnel2"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

The Name and Interface Settings

Step 4. Select “Remote Gateway (Static IP or Hostname)” for **Remote Settings** and then enter the gateway address of Company A.

Remote Settings	
<input checked="" type="radio"/> Remote Gateway (Static IP or Hostname) :	<input type="text" value="61.11.11.11"/> (Max. 80 characters)
<input type="radio"/> Remote Gateway or Client (Dynamic IP)	

The Remote Settings

Step 5. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of the string is 62 characters.)

Authentication Method :	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key String :	<input type="text" value="1234567890"/> (Max. 62 characters)

The Authentication Method Settings

Step 6. Under the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, select “MD5” for **Authentication Algorithm**, and then select “Diffie-Hellman 1” for **Key Group**.

Encryption and Data Integrity Algorithms Help	
ISAKMP Settings	
Encryption Algorithm :	<input type="text" value="3DES"/>
Authentication Algorithm :	<input type="text" value="MD5"/>
Key Group :	<input type="text" value="Diffie-Hellman 1"/>

The Encryption and Data Integrity Algorithms

Step 7. Select the radio box of “Use both algorithms” under the **IPSec Settings** section, select “3DES” for **Encryption Algorithm** and select “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

The IPSec Algorithm Settings

Step 8. In the **Advanced Settings (optional)** section, select “DH 1” for **PFS Key Group**, enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field, and then select “Main Mode” for **IKE Negotiation**.



PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

The Advanced Settings

Step 9. The IPSec autokey rule is successfully added.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	IPSec_tunnel2	WAN1	61.11.11.11	3DES / MD5	---	Modify Remove

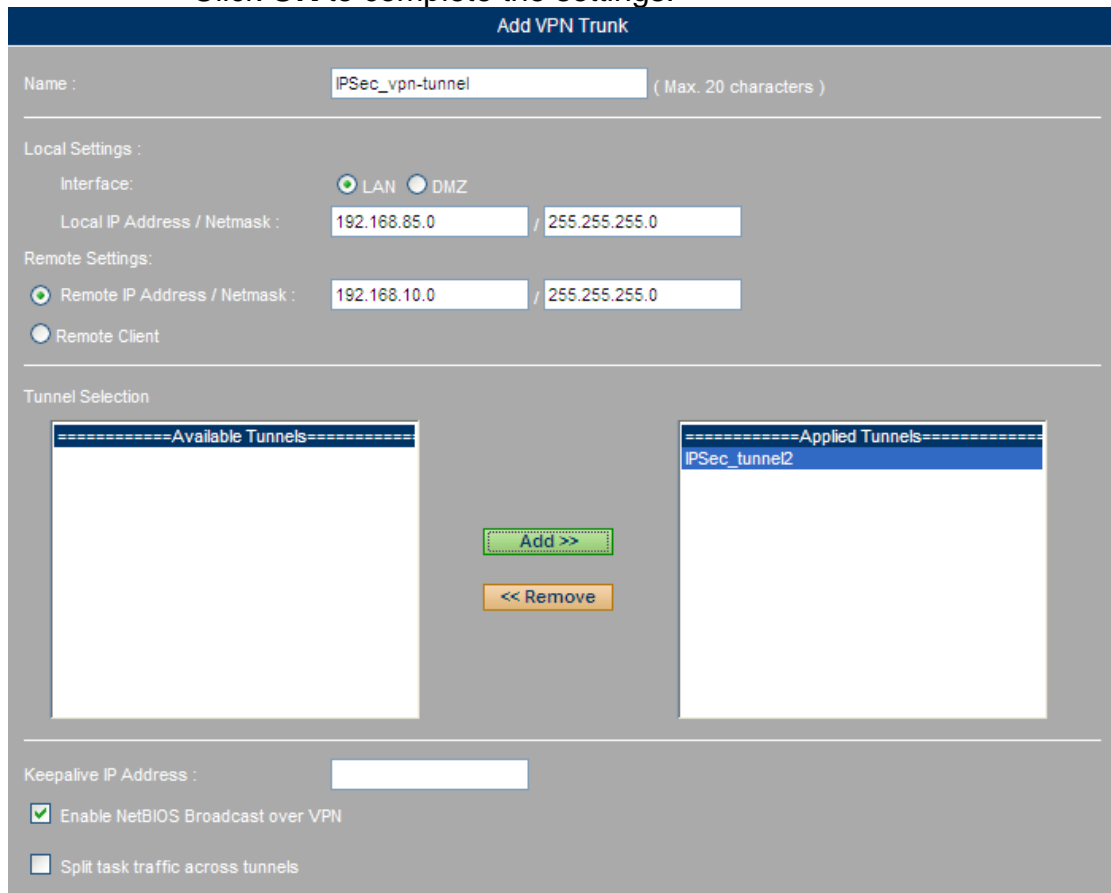
1 / 1 Go

Total entries : 1


[New Entry](#)

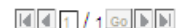
IPSec Autokey Rule Successfully Added

- Step 10. Under **Policy Object > VPN > Trunk**, set as shown below:
- **Name:** Specify a name for the VPN trunk.
 - **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask of Company B.
 - **Remote Settings:** Specify the subnet and netmask of Company A.
 - **Tunnel Selection:** Select “VPN_B” from the **Available Tunnels** column on the left, and then click **Add**.
 - Tick the box of “Enable NetBIOS Broadcast over VPN”.
 - Click **OK** to complete the settings.



Adding a VPN Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	IPSec_vpn-tunnel	192.168.85.0 / 24	192.168.10.0 / 24	IPSec_tunnel2	<div>Modify</div> <div>Remove</div>



New Entry

VPN Trunk Successfully Added

Step 11. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :	Inside Any
Destination Address :	Outside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	IPSec_vpn-tunnel

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

/ 1

Total entries : 1

Policy Successfully Created

Step 12. Under **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :

Outside Any

Destination Address :

Inside Any

Service :

Any

Schedule :

----- None -----

Authentication :

----- None -----

VPN Trunk :

IPSec_vpn-tunnel

Action :

☒ Permit connections from Incoming
 ☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

⚙️ Advanced Settings

OK

Cancel

Creating a Policy to Apply the VPN Trunk Settings

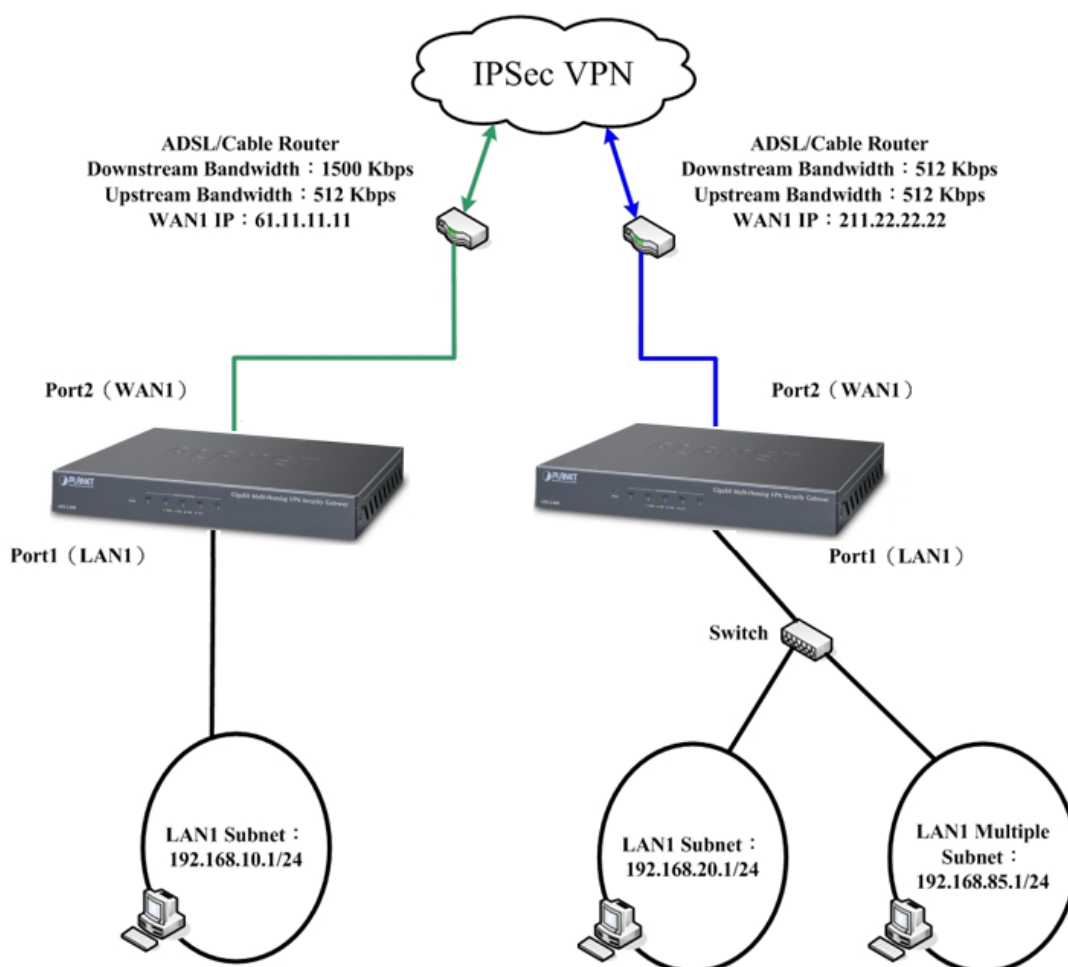
Source	Destination	Service	Action	Options					Configuration			Priority
Outside Any	Inside Any	Any	VPN						Modify	Remove	Pause	1

⏮ ⏪ ⏩ ⏭ / 1 ⏮ ⏪ ⏩ ⏭

New Entry

Policy Successfully Created

Step 13. IPSec VPN tunnel has been successfully established between the two sites.



The Deployment of an IPSec VPN Network between Two Units of MH-2300

4.8.1.2 Using a Unit of MH-2300 and a Windows 7 PC to Establish an IPSec VPN Tunnel

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Company A is running a unit of MH-2300 with the following configuration:
Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Company B is running a Windows 7 PC with an IP address of 211.22.22.22.

This example will be using a unit of MH-2300 and a Windows 7 PC to establish a VPN tunnel for private network access as follows.

For Company A, set as shown below:

Step 1. Go to **Policy Object > VPN > IPSec Autokey** and then click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
Sort by Name		No data found!				
New Entry						

The IPSec Autokey Rule Table

Step 2. Enter “VPN_A” in the **Name** field and then select “Port2 (WAN1)” for **Interface**.

Basic Settings (Required)	
Name :	<input type="text" value="ipsec1"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

Name and Interface Settings

Step 3. Select “Remote Gateway or Client (Dynamic IP)” for **Remote Settings**.

Remote Settings	
<input type="radio"/> Remote Gateway (Static IP or Hostname) :	<input type="text"/> (Max. 80 characters)
<input checked="" type="radio"/> Remote Gateway or Client (Dynamic IP)	

Remote Settings

Step 4. Select Pre-Shared Key from the **Authentication Method** drop-down list, and enter a string. (The maximum length of the string is 62 characters.)

Authentication Method :	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key String :	<input type="text" value="123456789"/> (Max. 62 characters)

Authentication Method Settings

Step 5. In the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, select “MD5” for **Authentication Algorithm**, and then select “Diffie-Hellman 2” for **Key Group**.

Encryption and Data Integrity Algorithms Help	
ISAKMP Settings	
Encryption Algorithm :	<input type="text" value="3DES"/>
Authentication Algorithm :	<input type="text" value="MD5"/>
Key Group :	<input type="text" value="Diffie-Hellman 2"/>

Encryption and Data Integrity Algorithms

Step 6. Select the radio box of “Use both algorithms” under the **IPSec Settings** section, select “3DES” for **Encryption Algorithm**, and then select “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 7. In the **Advanced Settings (Optional)** section, select “DH 1” for **PFS Key Group**, enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field, and then select “Main Mode” for **IKE Negotiation**.



PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

Advanced Settings

Step 8. The IPSec autokey rule is successfully added.

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
	ipsec1	WAN1	Dynamic IP	3DES / MD5	---	Modify Remove

1 / 1 Go

[New Entry](#)

IPSec Autokey Rule Successfully Added

Step 9. Under **Policy Object > VPN > Trunk**, set as shown below:

- **Name:** Specify a name for the VPN trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask of Company A.
- **Remote Settings:** Select **Remote Client**.
- **Tunnel Selection:** Select “VPN_A” from the **Available Tunnels** column on the left and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☐ Remote IP Address / Netmask : /

☒ Remote Client

Tunnel Selection

=====Available Tunnels=====

=====Applied Tunnels=====


ipsec1

Keepalive IP Address :

☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

Add a VPN Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	IPSec_vpn-tunnel	192.168.10.0 / 24	Remote Client	ipsec1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

/

VPN Trunk Successfully Added

- Step 10. Under **Policy > Outgoing**, set as shown below:
- Select the VPN trunk for **VPN Trunk**.
 - Click **OK**.

Add Policy

Source Address : Inside Any

Destination Address : Outside Any

Service : Any

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : IPSec_vpn-tunnel

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

⚙️ Advanced Settings

OK
Cancel

Creating a Policy to Apply the VPN Trunk Settings

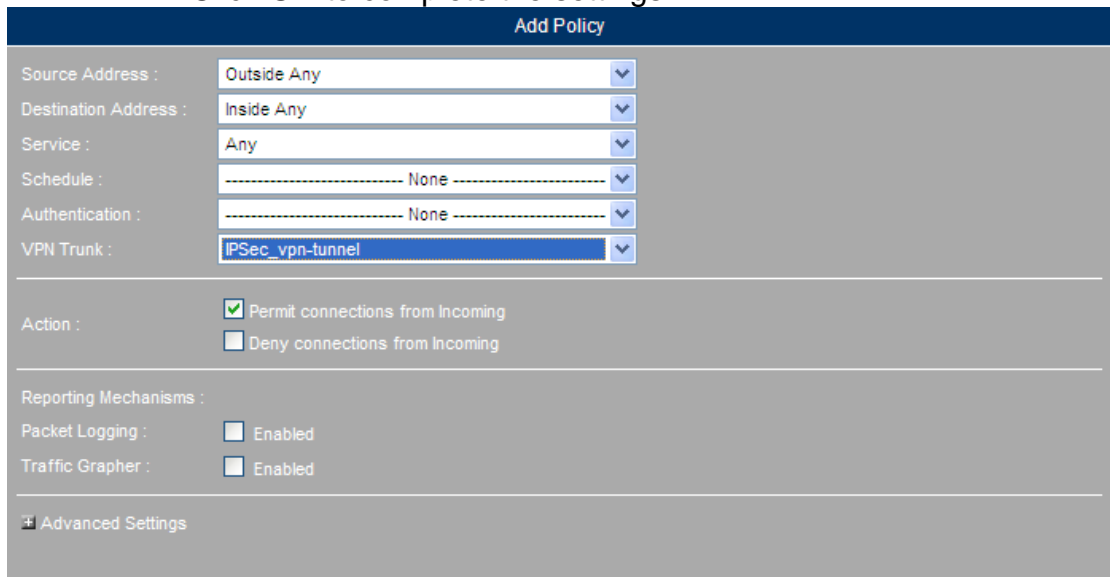
Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any	VPN									Modify	Remove	Pause	1

⏮ ⏪ ⏩ ⏭ / 1 ⏴ ⏵

New Entry

Policy Successfully Created

- Step 11. Under **Policy > Incoming**, set as shown below:
- Select the VPN trunk for **VPN Trunk**.
 - Click **OK** to complete the settings.



OK Cancel

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1

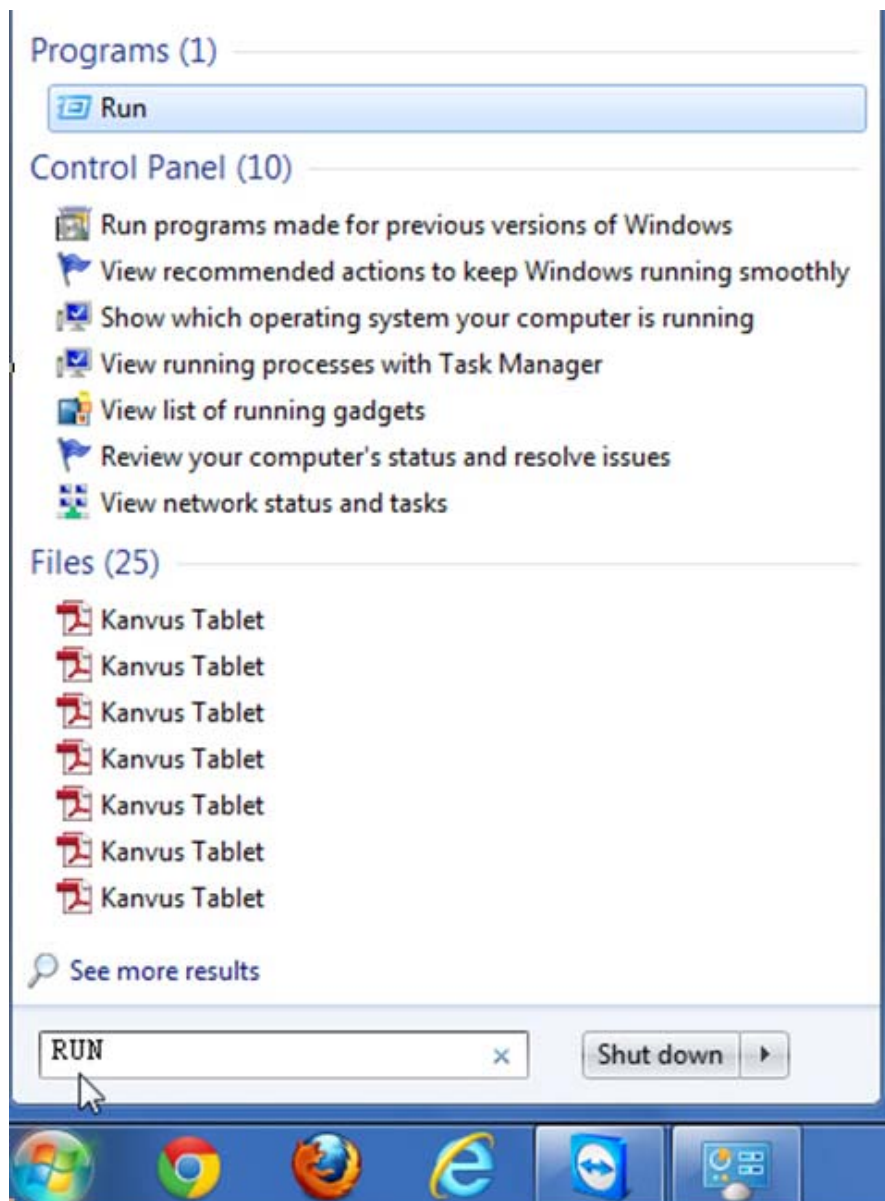
1 / 1

New Entry

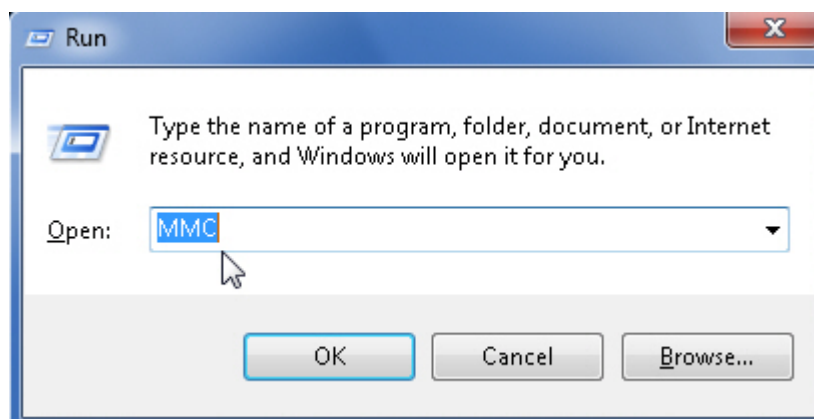
Policy Successfully Created

For B Company, set as shown below:

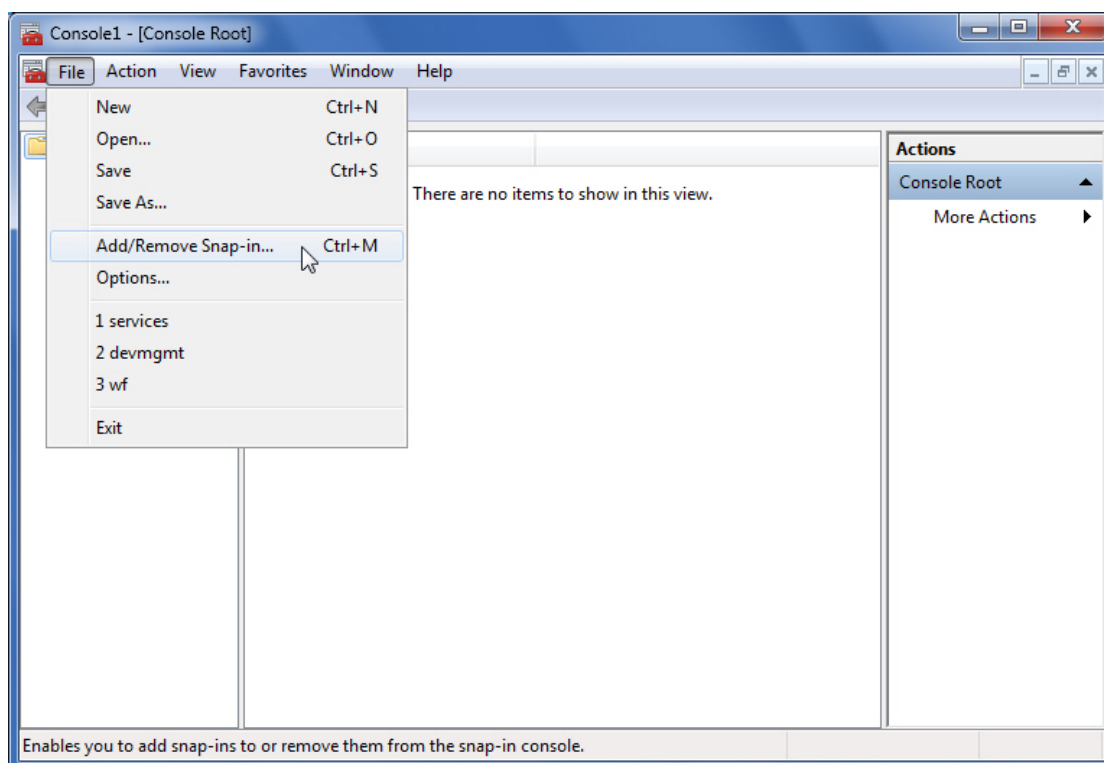
- Step 1. Type in “mmc” in the **Search** field on the **Start** menu or in the **Run** command box, and then set as shown below:
- Select “File” from the menu bar and then select “Add/Remove Snap-in”.
 - In the **Add or Remove Snap-ins** window, follow the steps below :
 - Select “IP Security Policy Management” from the **Available snap-ins** column on the left, and then click **Add**.
 - Tick the radio box of “Local Computer”, and then click **Finish**.
 - Click **OK** to complete the settings.
 - In the **Console Root** tree, right-click **IP Security Policies on Local Computer** and then click **Create IP Security Policy**.
 - In the **IP Security Policy Wizard** window, follow the steps below:
 - Click **Next**.
 - Type in “VPN_B” in the **Name** field.
 - Click **Next**.
 - Click **Next**.
 - Tick the box of “Edit properties” and then click **Finish**.



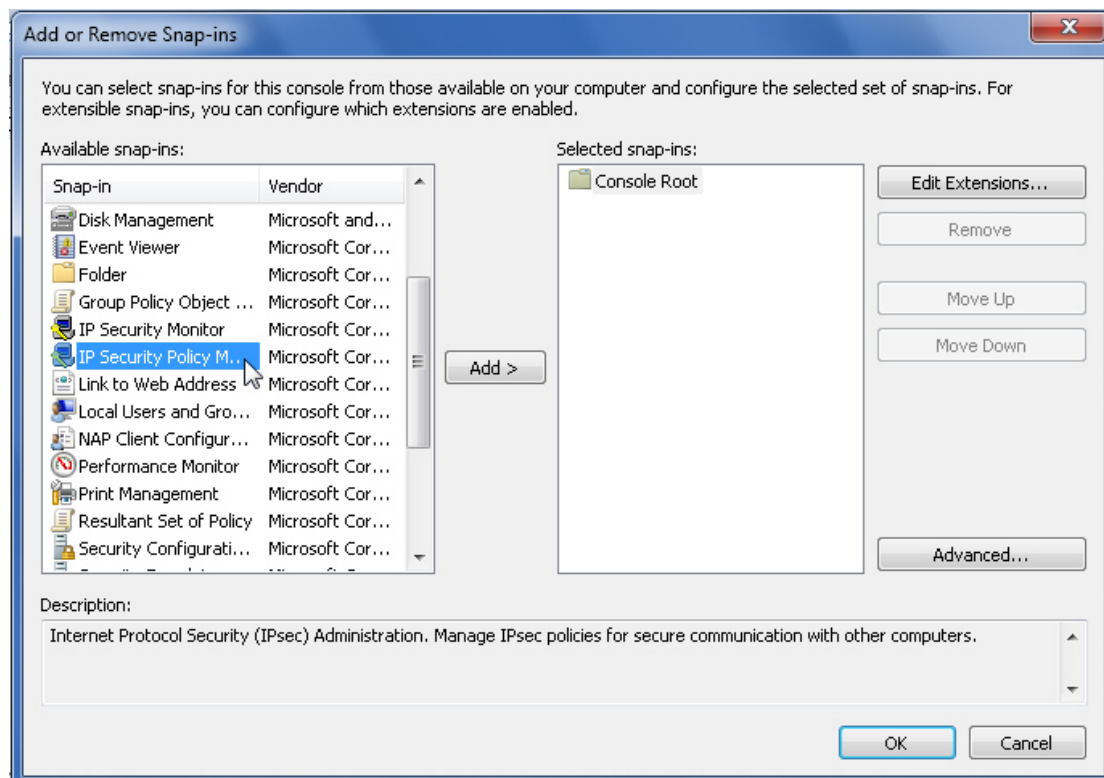
Typing in "run" in the Search Field on the Start Menu



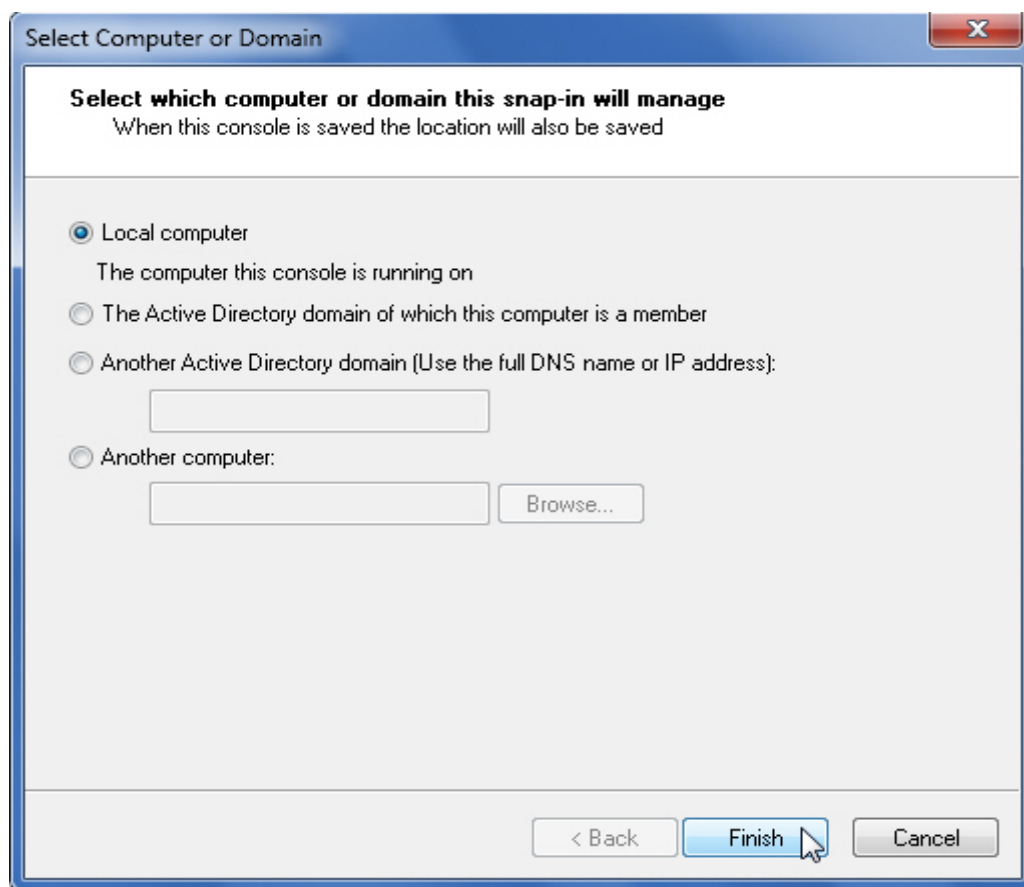
Typing in "mmc" in the Run Command Box



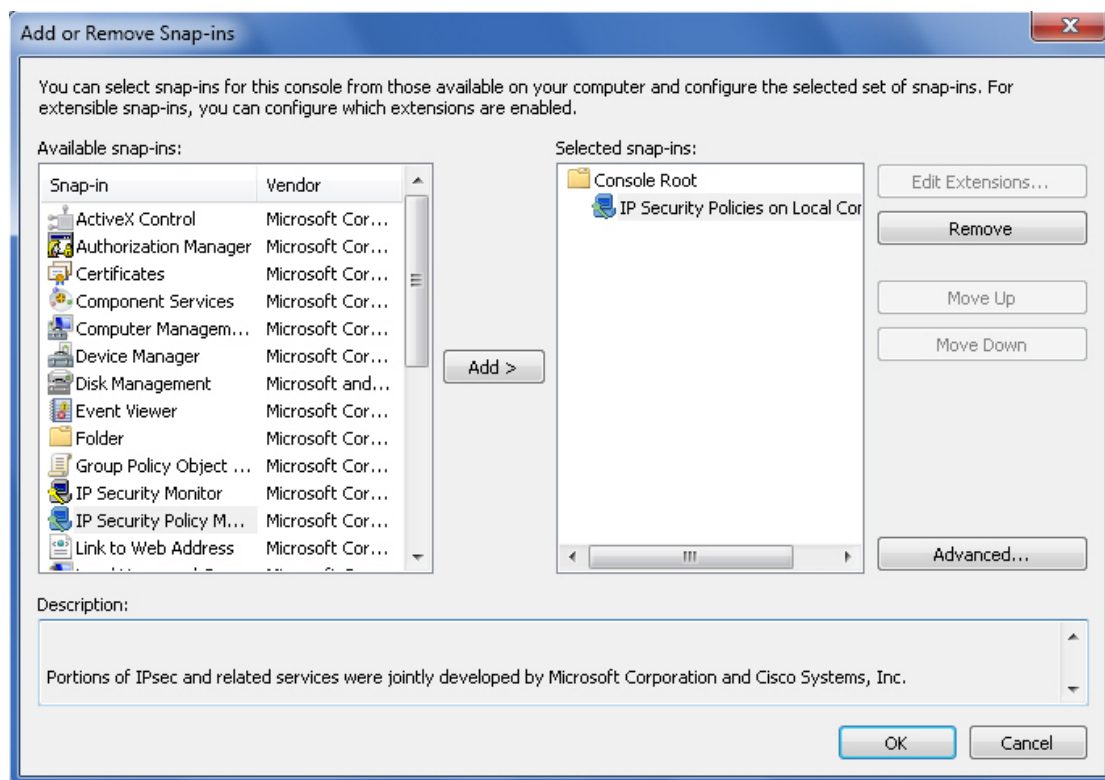
Selecting “Add / Remove Snap-in” from the File Menu



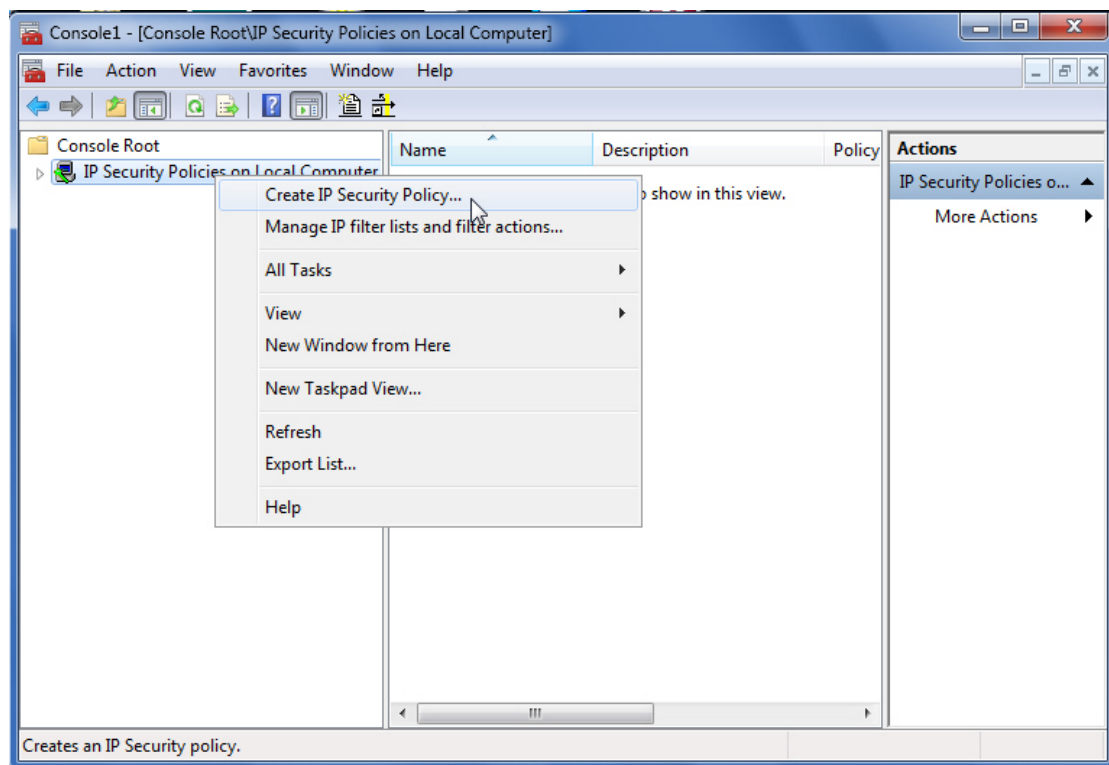
Adding the “IP Security Policy Management”



Selecting "Local Computer"



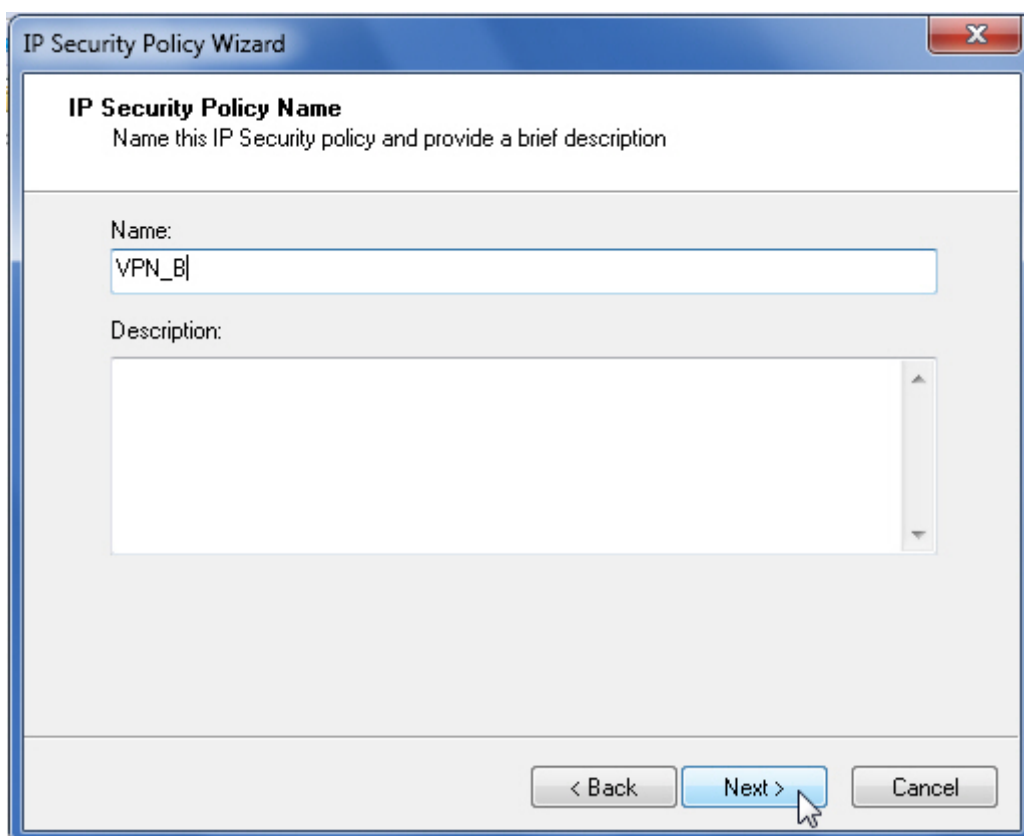
Snap-in Successfully Added to the Console Root



Creating an IP Security Policy

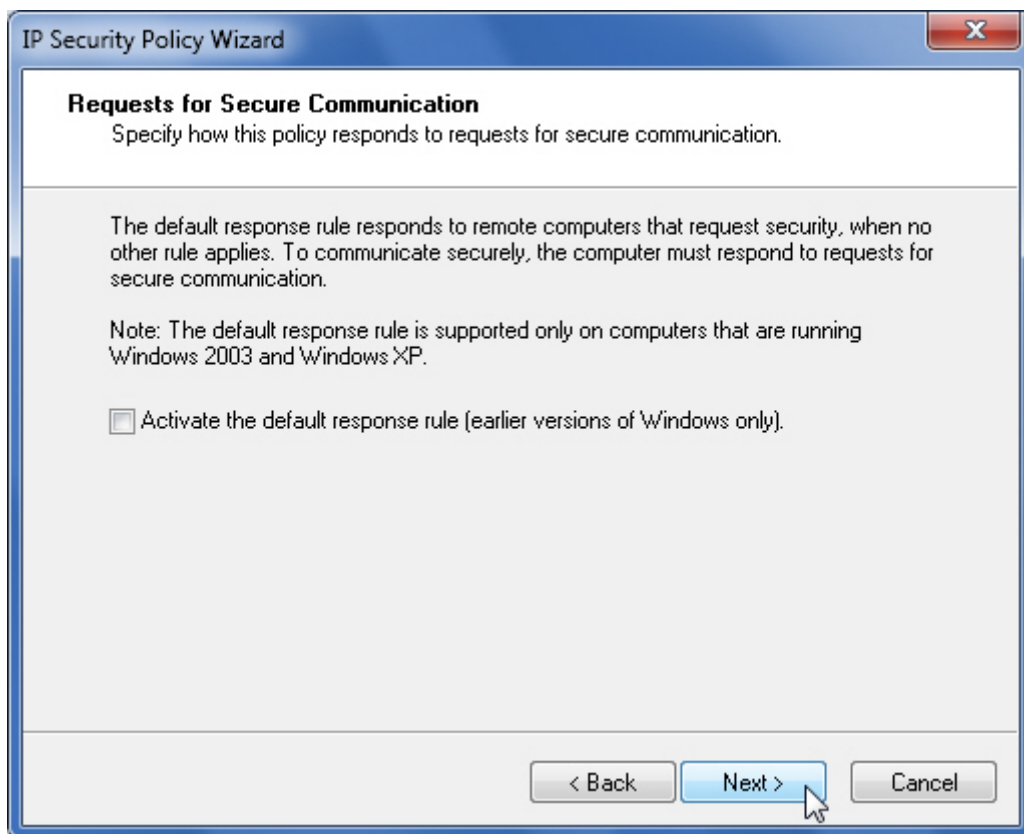


The IP Security Policy Wizard



The screenshot shows the 'IP Security Policy Wizard' window. The title bar says 'IP Security Policy Wizard'. The main heading is 'IP Security Policy Name'. Below it, the instruction reads: 'Name this IP Security policy and provide a brief description'. There are two input fields: 'Name:' with the text 'VPN_B' entered, and 'Description:' which is an empty text area. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Policy Name and Description Settings



The screenshot shows the 'IP Security Policy Wizard' window at the 'Requests for Secure Communication' step. The title bar says 'IP Security Policy Wizard'. The main heading is 'Requests for Secure Communication'. Below it, the instruction reads: 'Specify how this policy responds to requests for secure communication.' There is a paragraph of text: 'The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.' Below this is a note: 'Note: The default response rule is supported only on computers that are running Windows 2003 and Windows XP.' At the bottom, there is a checkbox labeled 'Activate the default response rule (earlier versions of Windows only)'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Default Response Rule Settings

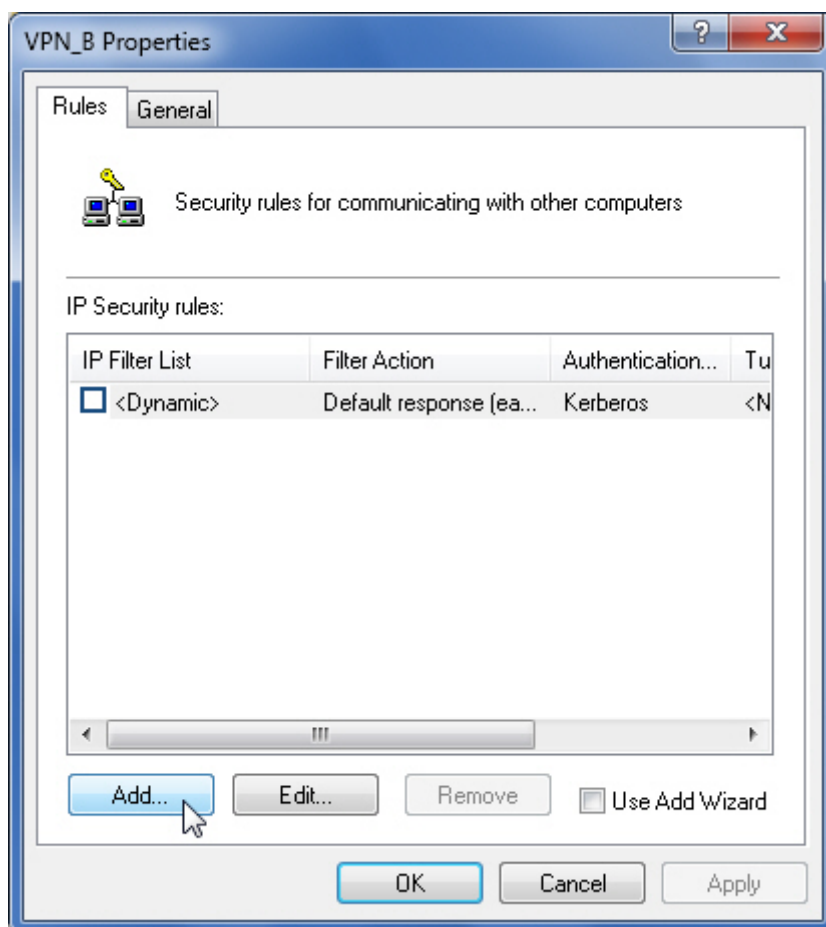


IP Security Policy Wizard Successfully Completed

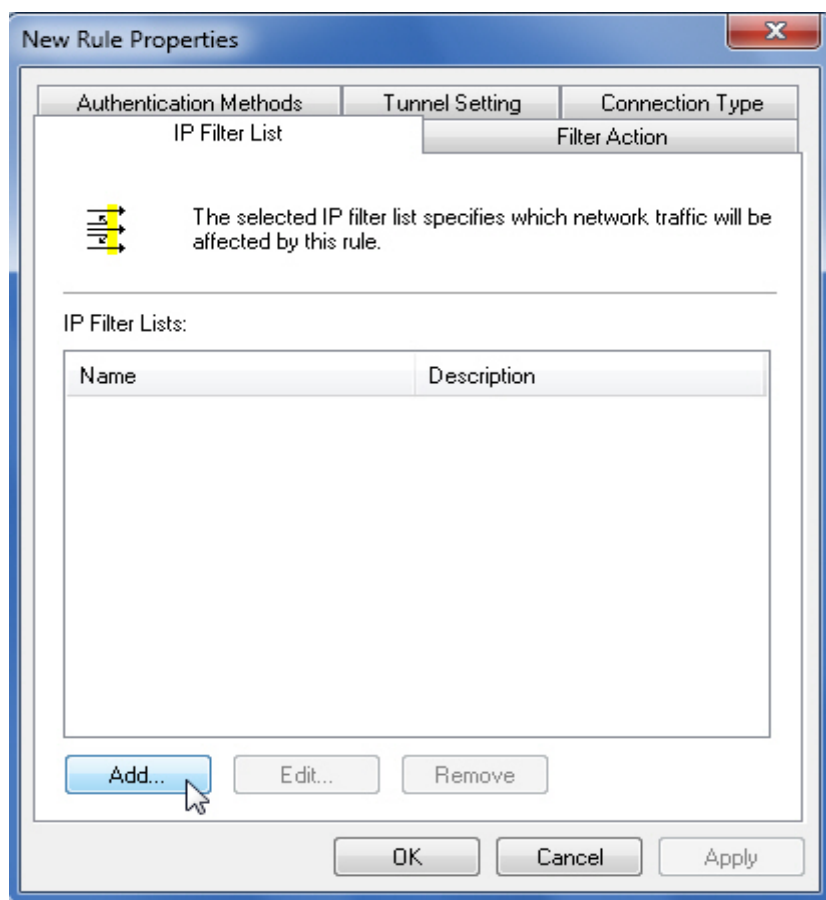
Step 2. In the **VPN_B Properties** dialog box, click the **Rules** tab and then set as shown below:

- Untick the box of "Use Add Wizard" and click **Add**.
- In the **New Rule Properties** dialog box, click the **IP Filter List** tab and then click **Add**:
 - ◆ In the **IP Filter List** dialog box, type "VPN_B Local To Remote" in the **Name** field and then click **Add**:
 - In the **IP Filter Properties** dialog box, click the **Addresses** tab:
 - **Source address**: Select "A specific IP Address or Subnet" and specify the corresponding IP address or subnet, ie., 211.22.22.22/32.
 - **Destination address**: Select "A specific IP Address or Subnet" and specify the corresponding IP address or subnet, i.e., 192.168.10.0/24.
 - Click **OK**.
 - Click **OK** to complete the settings.
 - ◆ Select "VPN_B Local To Remote" from **IP Filter Lists**.
- In the **New Rule Properties** dialog box, click the **Filter Action** tab, untick the box of "Use Add Wizard" and then click **Add**:
 - ◆ In the **New Filter Action Properties** dialog box, click the **Security Methods** tab and then set as shown below:
 - Select the radio box of "Negotiate security".

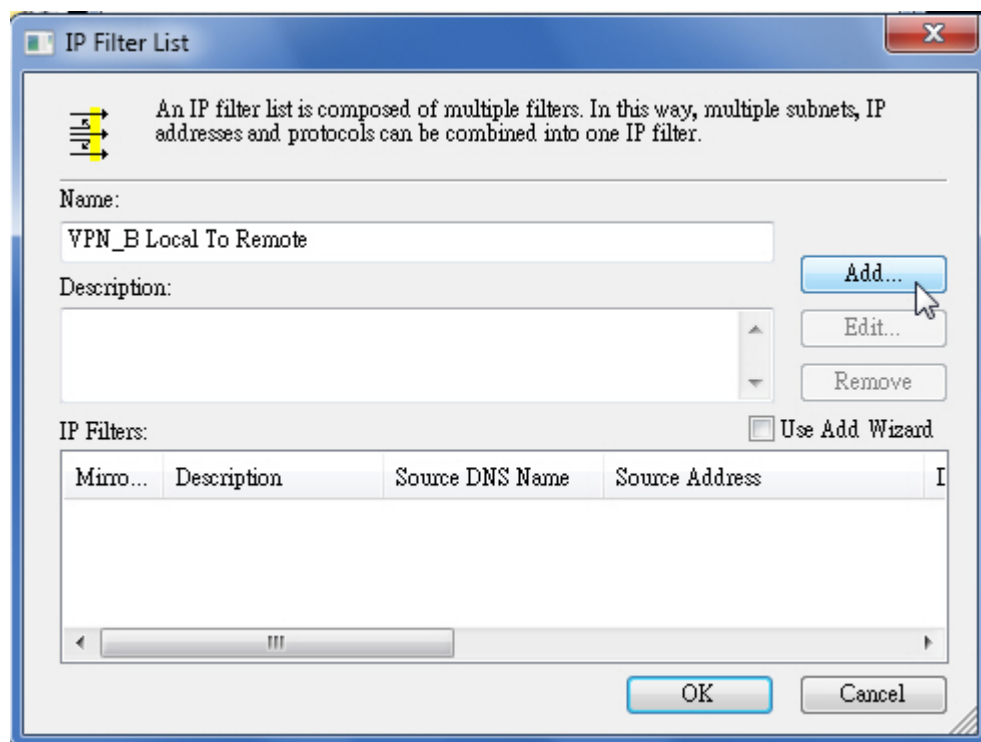
- Tick the boxes of “Accept unsecured communication, but always respond using IPsec” and “Use session key perfect forward secrecy (PFS)”.
- Click **Add**.
- In the **New Security Method** dialog box, select **Custom** and then click **Settings**.
 - In the **Custom Security Method Settings** dialog box, follow the steps below:
 - ✧ Tick the box of “Data integrity and encryption (ESP)”.
 - ✧ **Integrity algorithm**: Select “MD5”.
 - ✧ **Encryption algorithm**: Select “3DES”.
 - ✧ Under the **Session key settings** section, type in “3600” in the **seconds** field for the key generation interval.
 - ✧ Click **OK**.
 - Click **OK**.
- Click **OK** to complete the settings.
- ◆ Select “New Filter Action” from the **Filter Actions**.
- In the **New Rule Properties** dialog box, click the **Authentication Methods** tab. Next, select “Kerberos” from the **Authentication method preference order** and then click **Edit**.
 - ◆ In the **Edit Authentication Method Properties** dialog box, follow the steps below:
 - Tick the box of “Use this string (preshared key)” and enter “123456789” in the corresponding field.
 - Click **OK** to complete the settings.
 - ◆ Select “Preshared Key” from the **Authentication method preference order**.
- In the **New Rule Properties** dialog box, click the **Tunnel Setting** tab:
 - ◆ Select the radio box of “Tunnel endpoints are specified by these IP addresses”.
 - ◆ Specify the IPv4 tunnel endpoint. i.e., 61.11.11.11.
- In the **New Rule Properties** dialog box, click the **Connection Type** tab:
 - ◆ Tick the box of “**All network connections**”.
 - ◆ Click **Apply**.
 - ◆ Click **OK** to complete the settings.
- Select “VPN_B Local To Remote” from the **IP Security rules**.



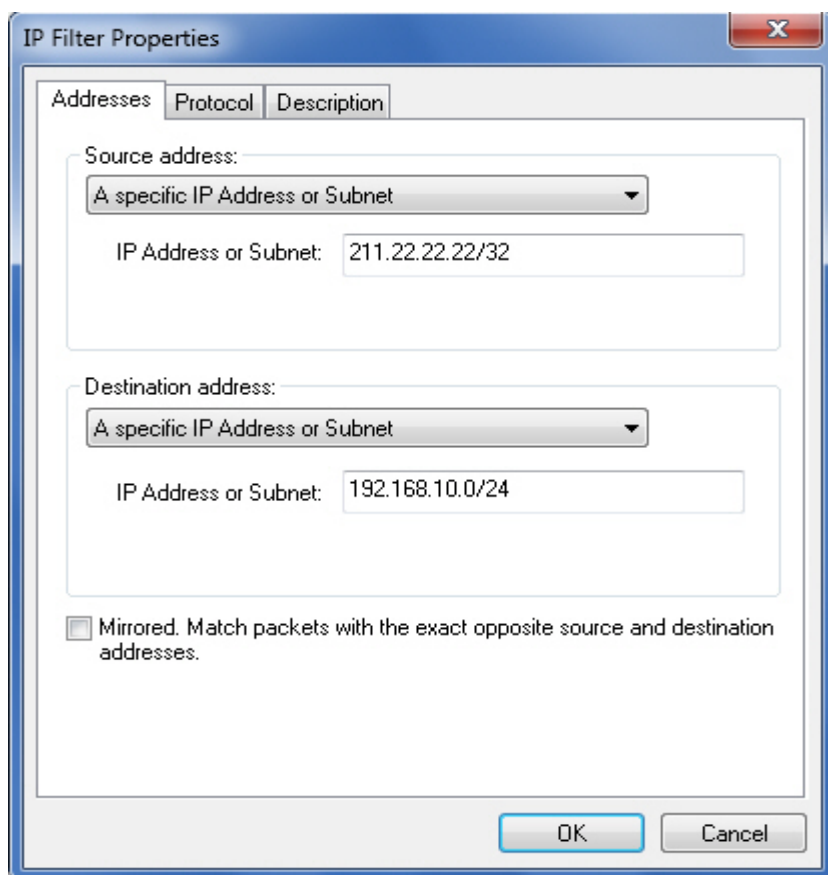
Adding an IP Security Rule



Adding an IP Filter List



Specifying a Name of the IP Filter List



The **IP Filter Properties** dialog box has three tabs: **Addresses**, **Protocol**, and **Description**. The **Addresses** tab is active.

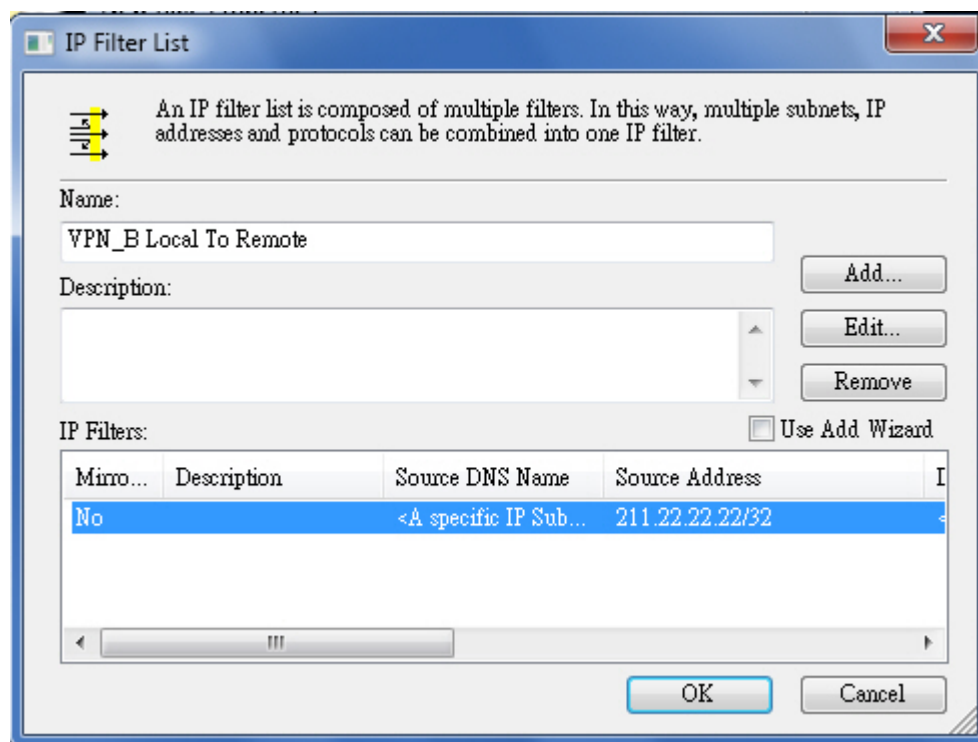
Source address:
 A specific IP Address or Subnet (dropdown menu)
 IP Address or Subnet: 211.22.22.22/32

Destination address:
 A specific IP Address or Subnet (dropdown menu)
 IP Address or Subnet: 192.168.10.0/24

☐ Mirrored. Match packets with the exact opposite source and destination addresses.

Buttons: **OK**, **Cancel**

Specifying the Source and Destination Addresses



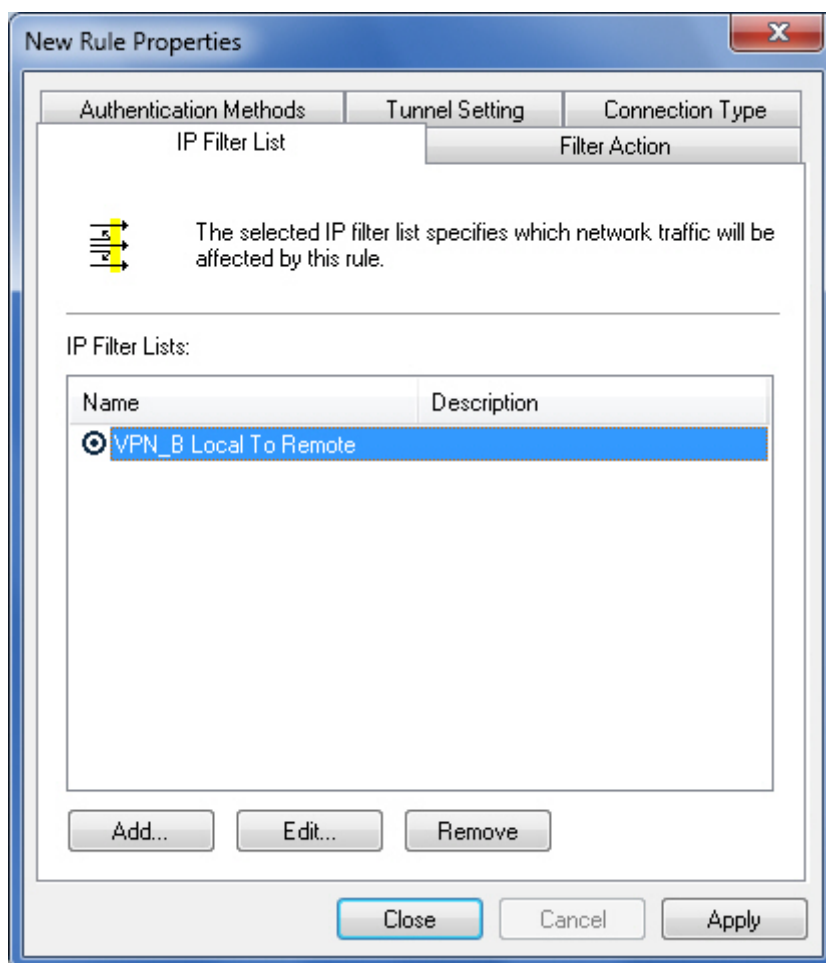
The **IP Filter List** dialog box contains the following elements:

- Icon:** A yellow arrow pointing right.
- Text:** An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.
- Name:** VPN_B Local To Remote
- Description:** (Empty text box)
- Buttons:** **Add...**, **Edit...**, **Remove**
- IP Filters:**
 - ☐ Use Add Wizard
 - Table with columns: **Mirro...**, **Description**, **Source DNS Name**, **Source Address**

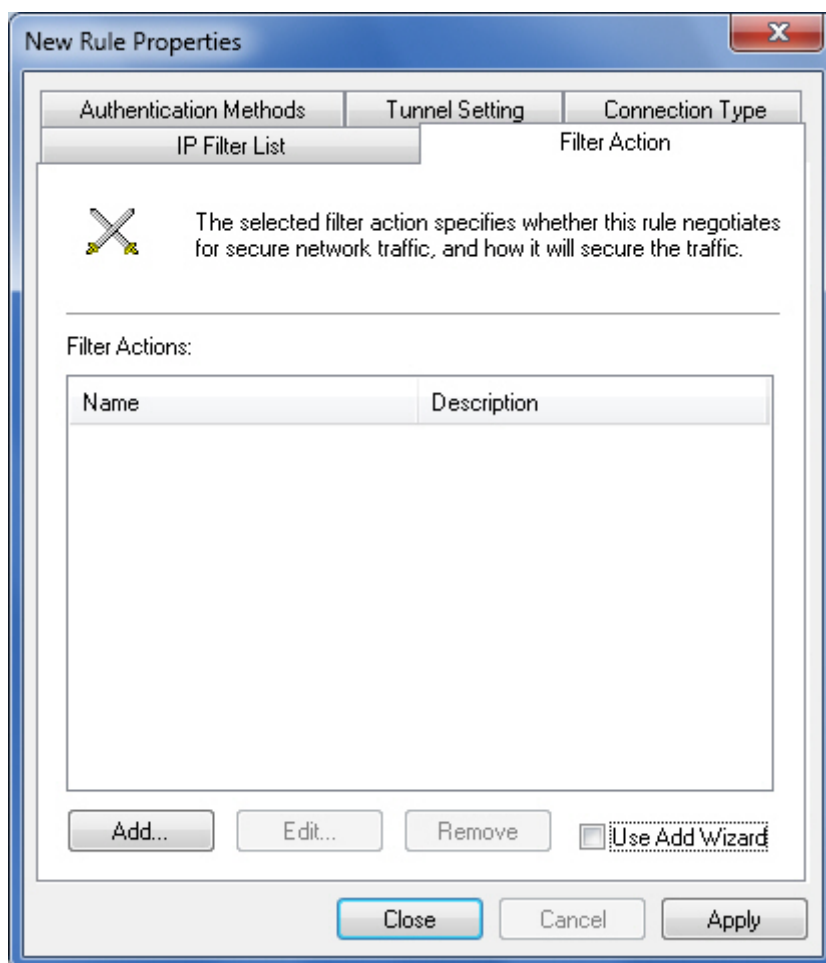
Mirro...	Description	Source DNS Name	Source Address
No	<A specific IP Sub...		211.22.22.22/32

Buttons: **OK**, **Cancel**

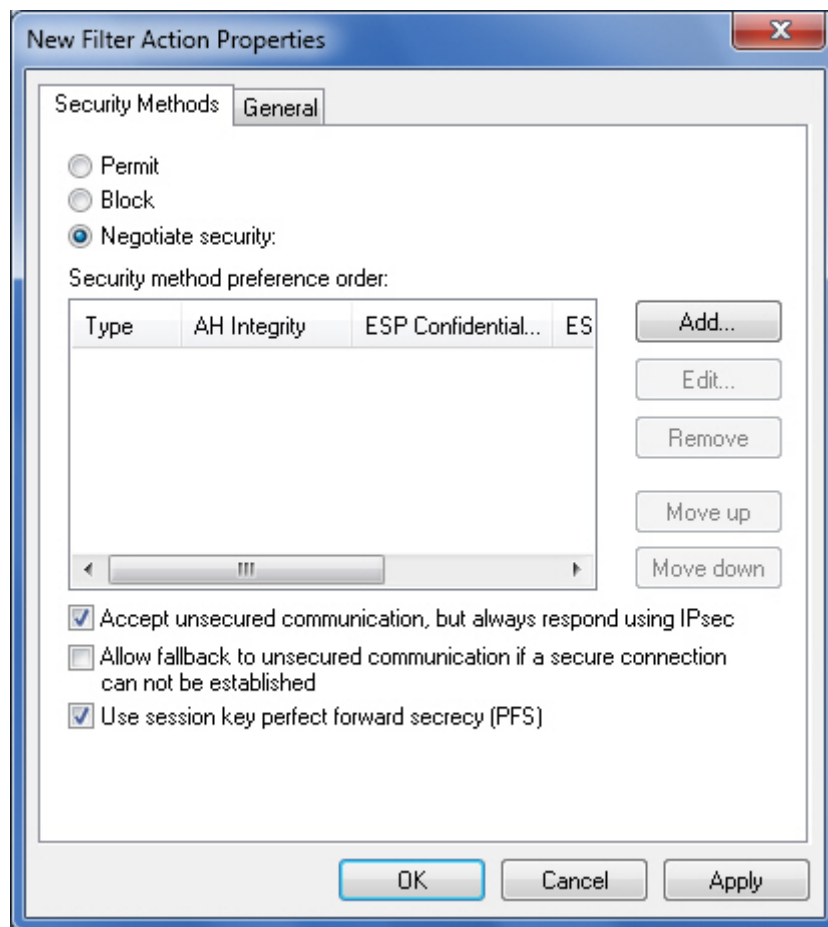
An IP Filter Successfully Added to the List



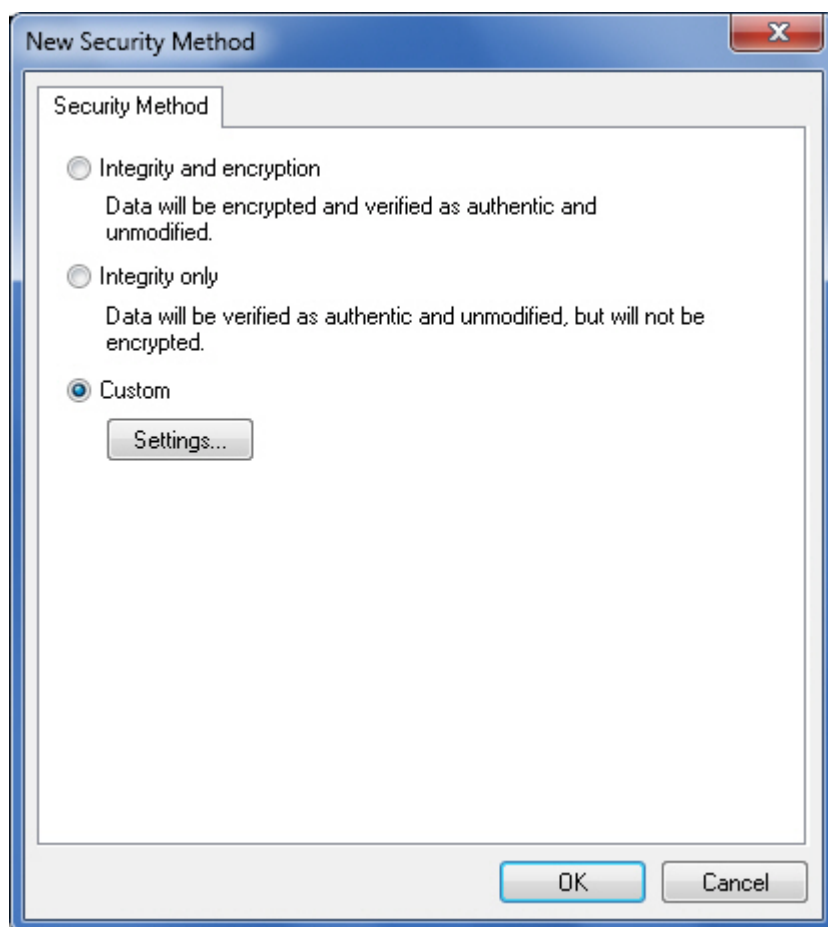
An IP Filter List Successfully Added to the Rule



Adding a Filter Action



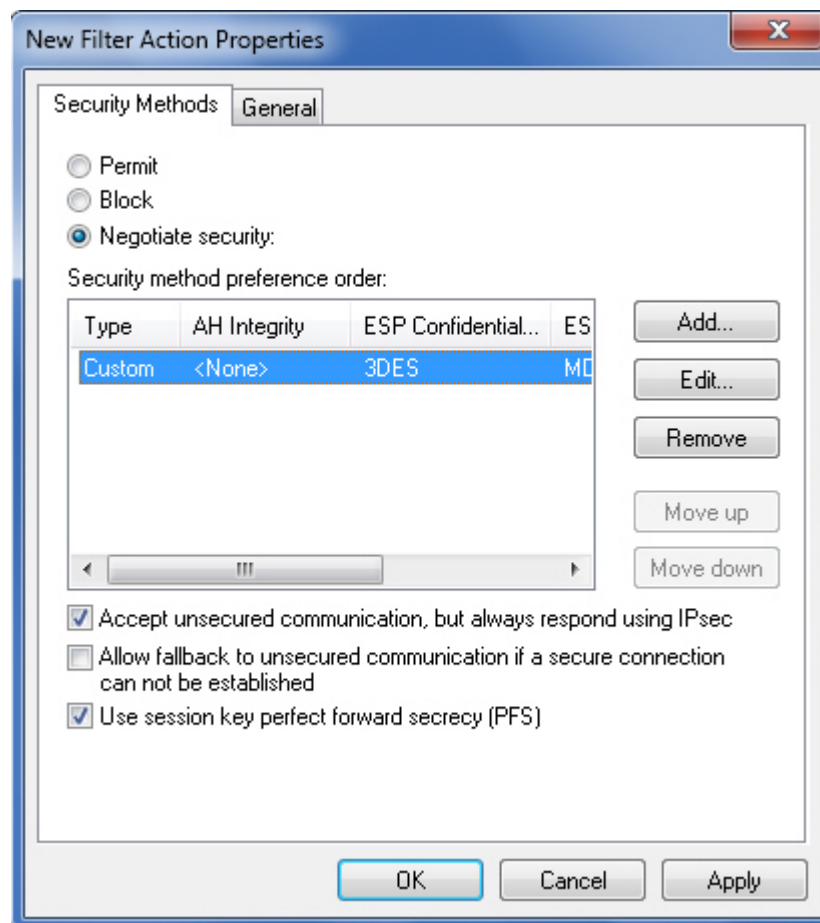
Configuring the Security Method



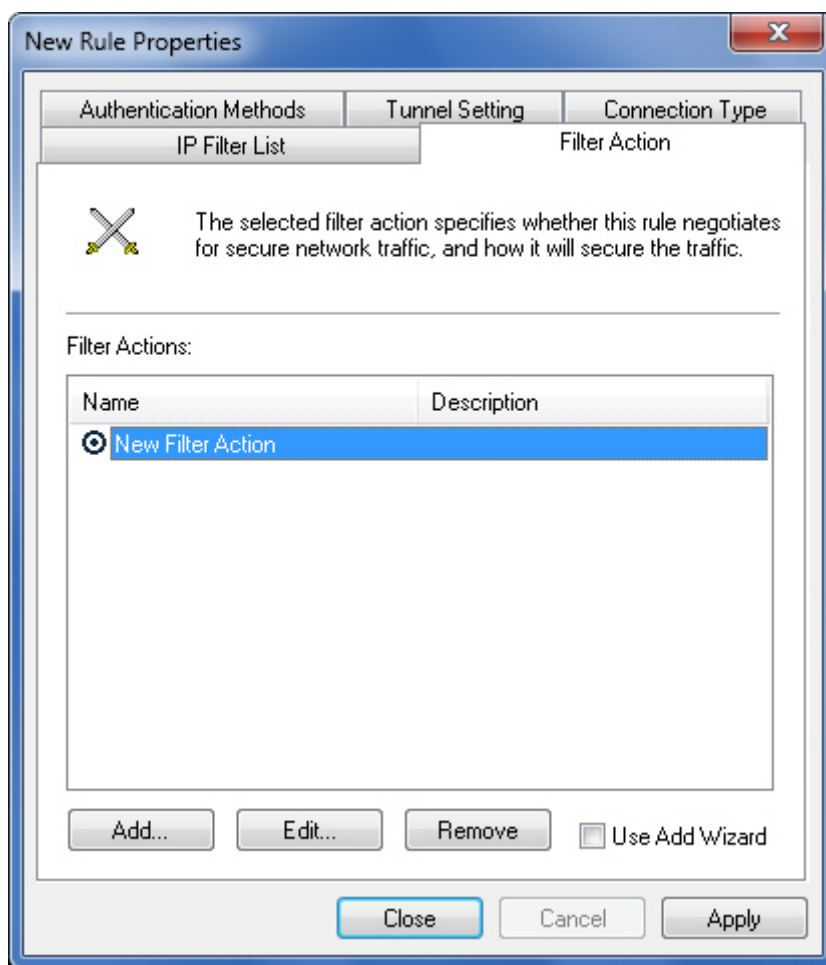
Customizing the Security Method



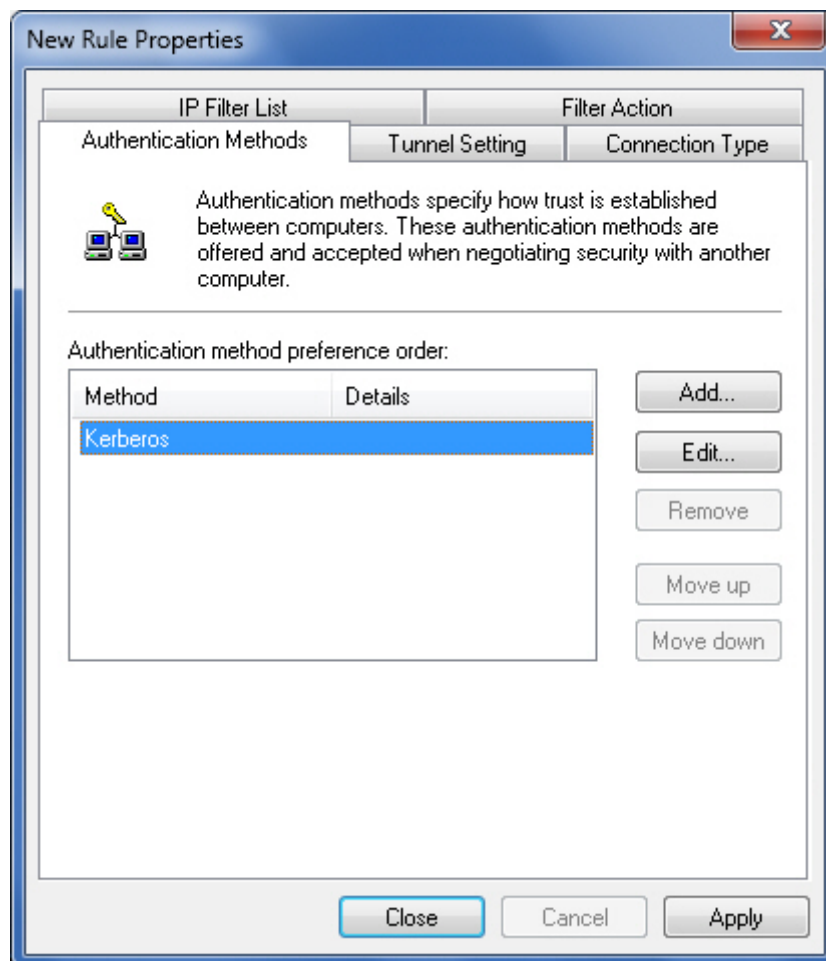
Specifying the Custom Security Method Settings



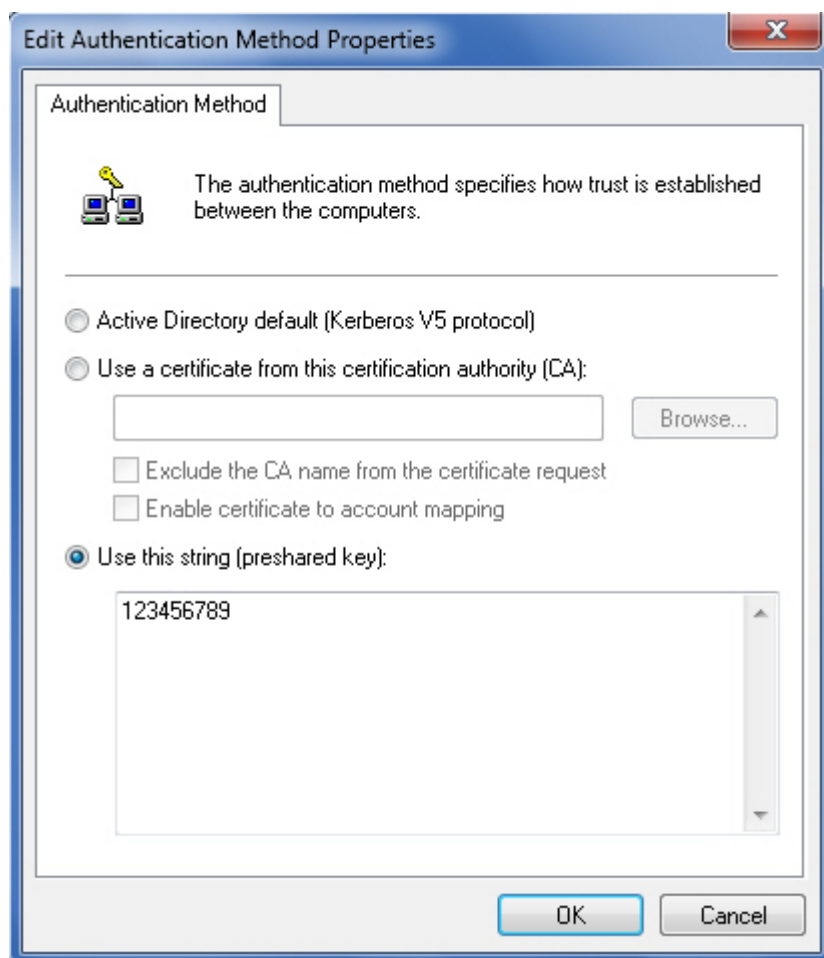
Security Method Settings Successfully Completed



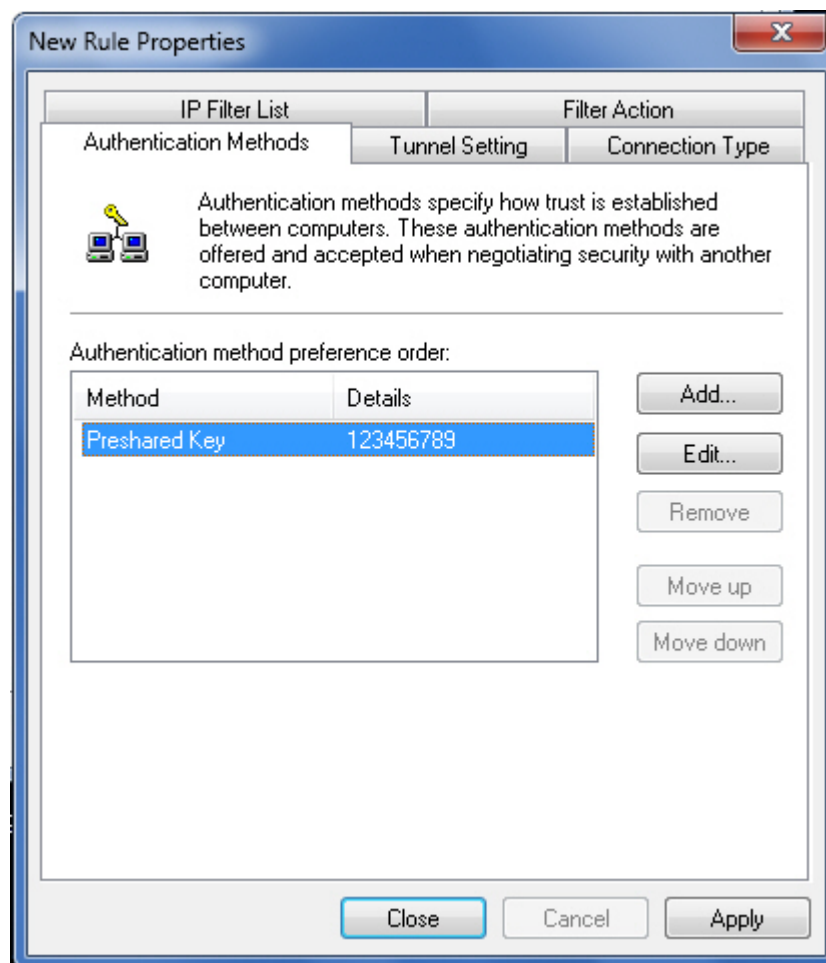
Filter Action Successfully Added to the Rule



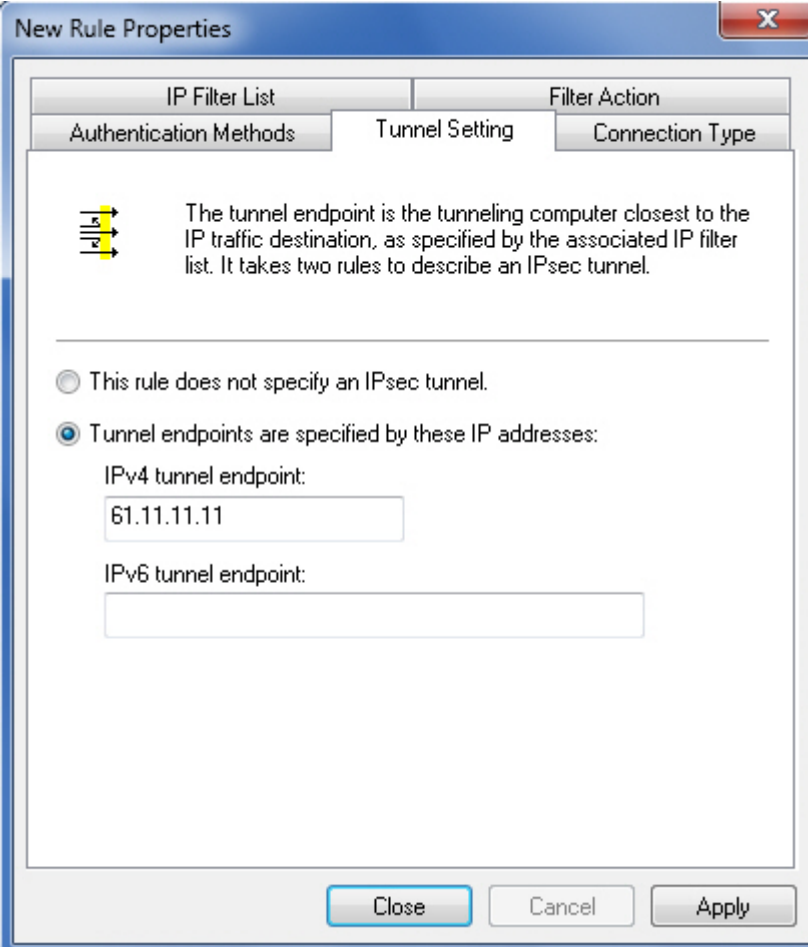
Editing the Authentication Method



Specifying a Preshared Key




Authentication Method Successfully Added to the Rule



New Rule Properties

IP Filter List | Filter Action

Authentication Methods | **Tunnel Setting** | Connection Type


 The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPsec tunnel.

☐ This rule does not specify an IPsec tunnel.

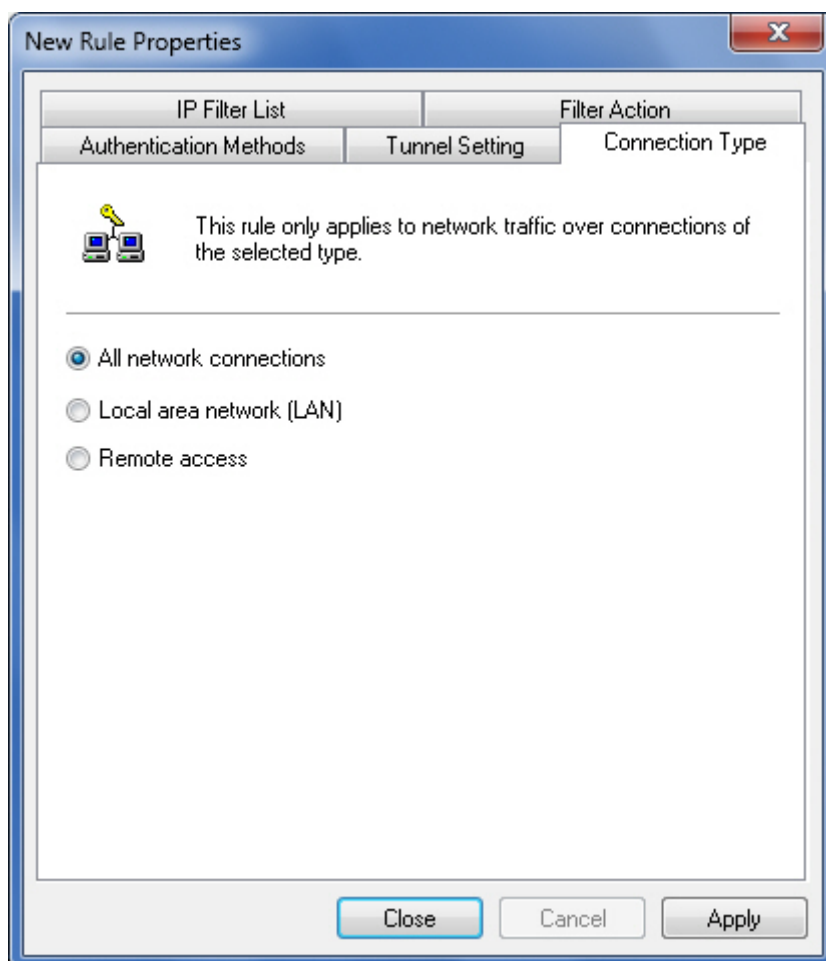
☒ Tunnel endpoints are specified by these IP addresses:

IPv4 tunnel endpoint:

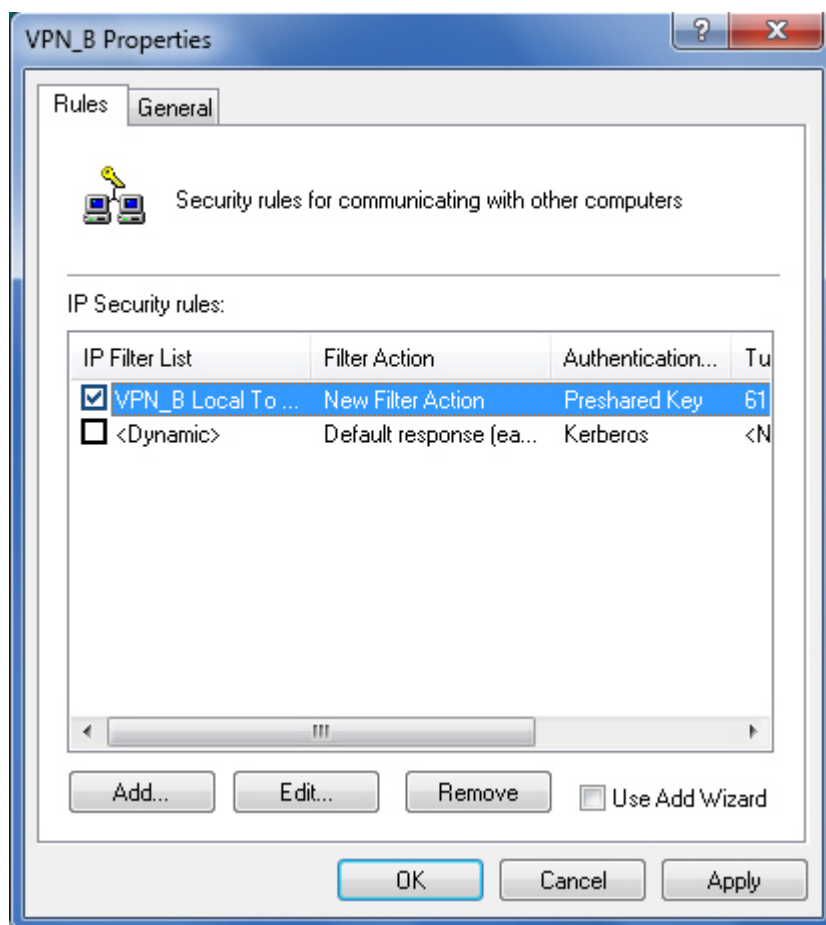
IPv6 tunnel endpoint:

Close Cancel Apply

Specifying the IPv4 Tunnel Endpoint



Applying the Rule to All Network Connections

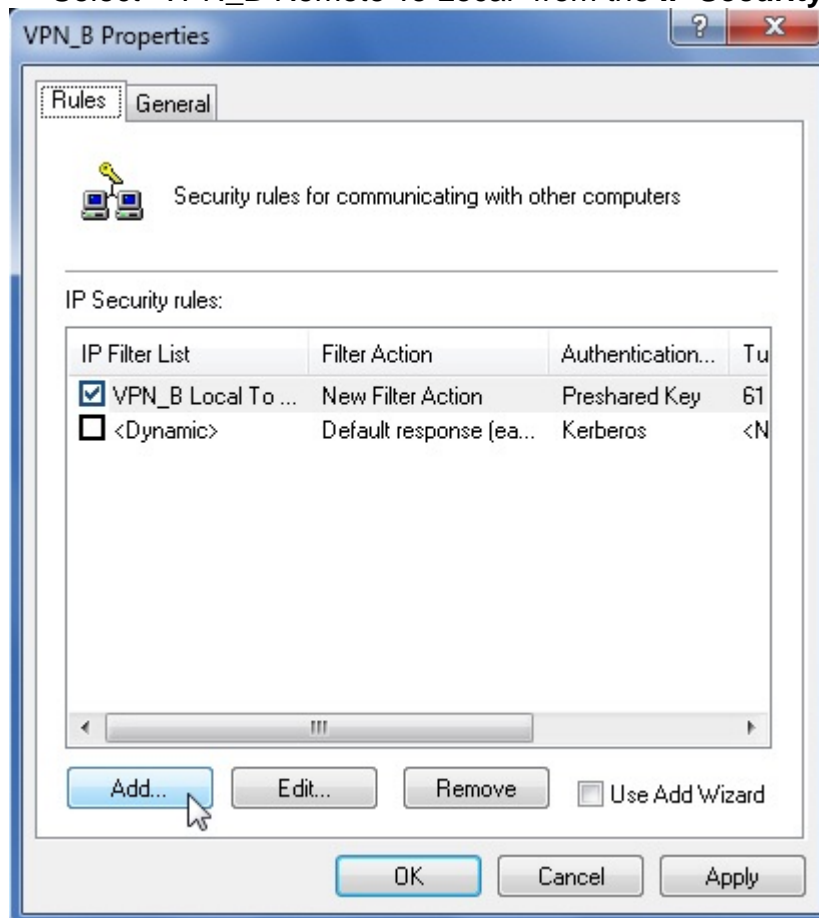


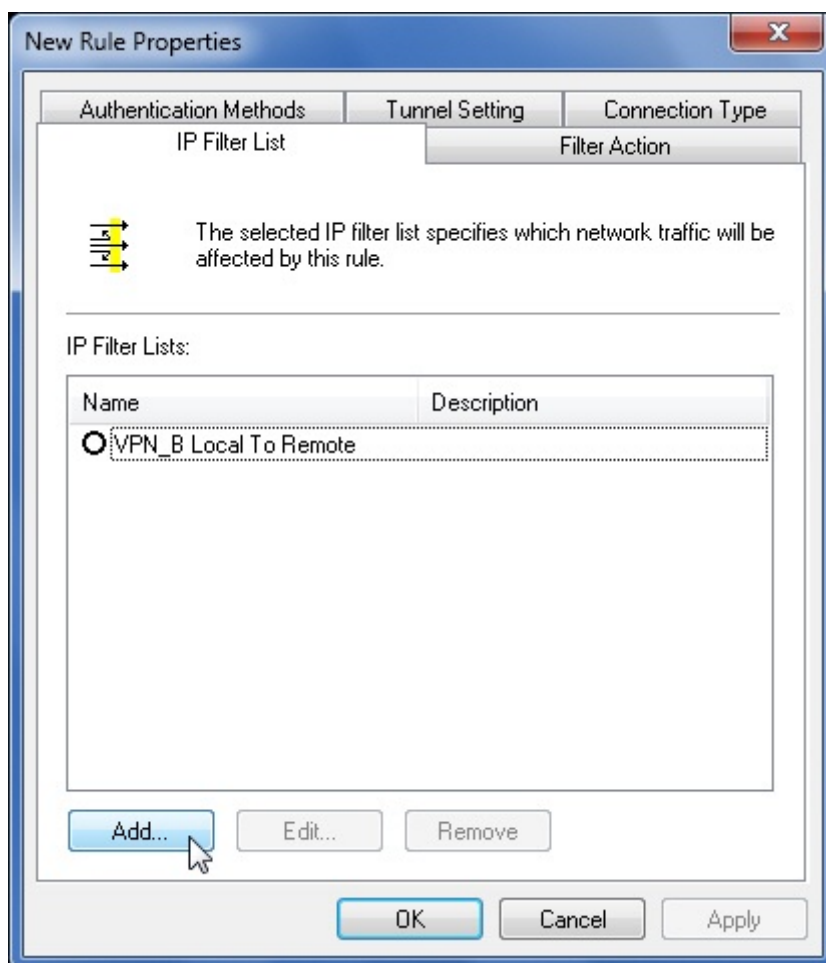
IP Security Rule Successfully Added

Step 3. In the **VPN_B Properties** dialog box, click the **Rules** tab and then set as shown below:

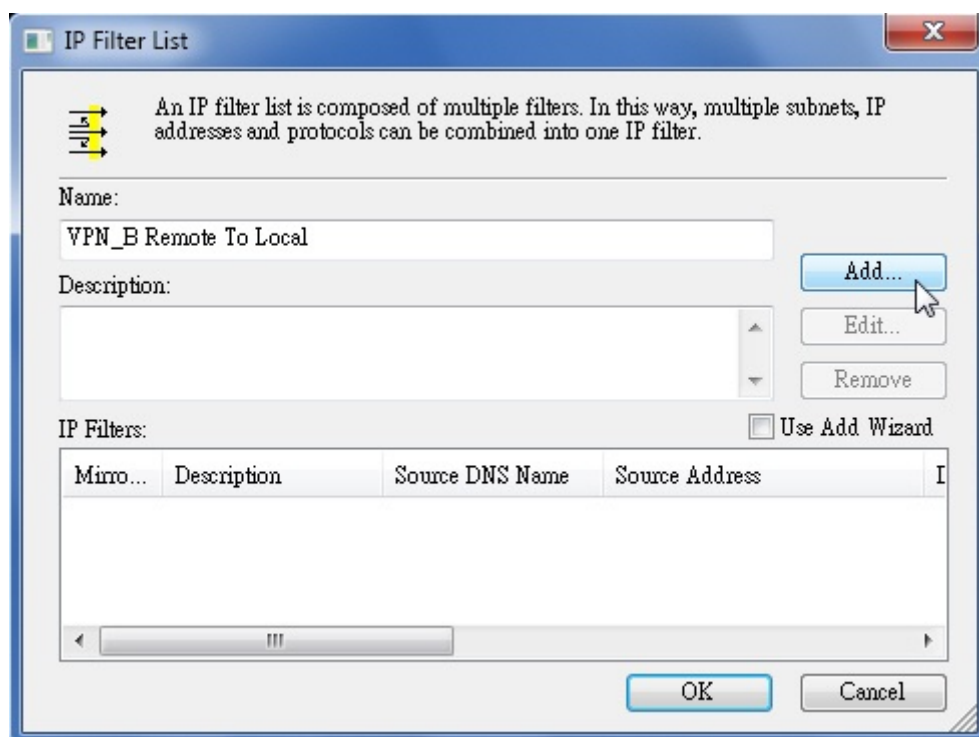
- Click **Add**.
- In the **New Rule Properties** dialog box, select the **IP Filter List** tab and then click **Add**:
 - ◆ In the **IP Filter List** dialog box, type in “VPN_B Remote To Local” in the **Name** field and then click **Add**:
 - In the **IP Filter Properties** dialog box, click the **Addresses** tab:
 - **Source address**: Select “A specific IP Address or Subnet” and specify the corresponding IP address or subnet, i.e., 192.168.10.0/24.
 - **Destination address**: Select “A specific IP Address or Subnet” and specify the corresponding IP address or subnet, i.e., 211.22.22.22/32.
 - Click **OK**.
 - Click **OK** to complete the settings.
 - ◆ Select “VPN_B Remote To Local” from the **IP Filter Lists**.
 - ◆ In the **New Rule Properties** dialog box, click the **Filter Action** tab, untick the box of “Use Add Wizard”, and then click **Add**.

- In the **New Rule Properties** dialog box, click the **Authenticaiton Methods** tab. Next, select “Kerberos” from the **Authethication method preference order** and then click **Edit**.
 - ◆ In the **Edit Authentication Method Properties** dialog box, follow the steps below:
 - Tick the box of “Use this string (presared key)” and enter “123456789” in the corresponding field.
 - Click **OK** to complete the settings.
 - ◆ Select “Preshared Key” from the **Authentication method preference order**.
- In the **New Rule Properties** dialog box, click the **Tunnel Setting** tab:
 - ◆ Select the radio box of “Tunnel endpoints are specified by these IP addresses”.
 - ◆ Specify the IPv4 tunnel endpoint, i.e., 211.22.22.22.
- In the **New Rule Properties** dialog box, click the **Connection Type** tab:
 - ◆ Tick the box of “**All network connections**”.
 - ◆ Click **Apply**.
 - ◆ Click **OK** to complete the settings.
- Select “VPN_B Remote To Local” from the **IP Security rules**.

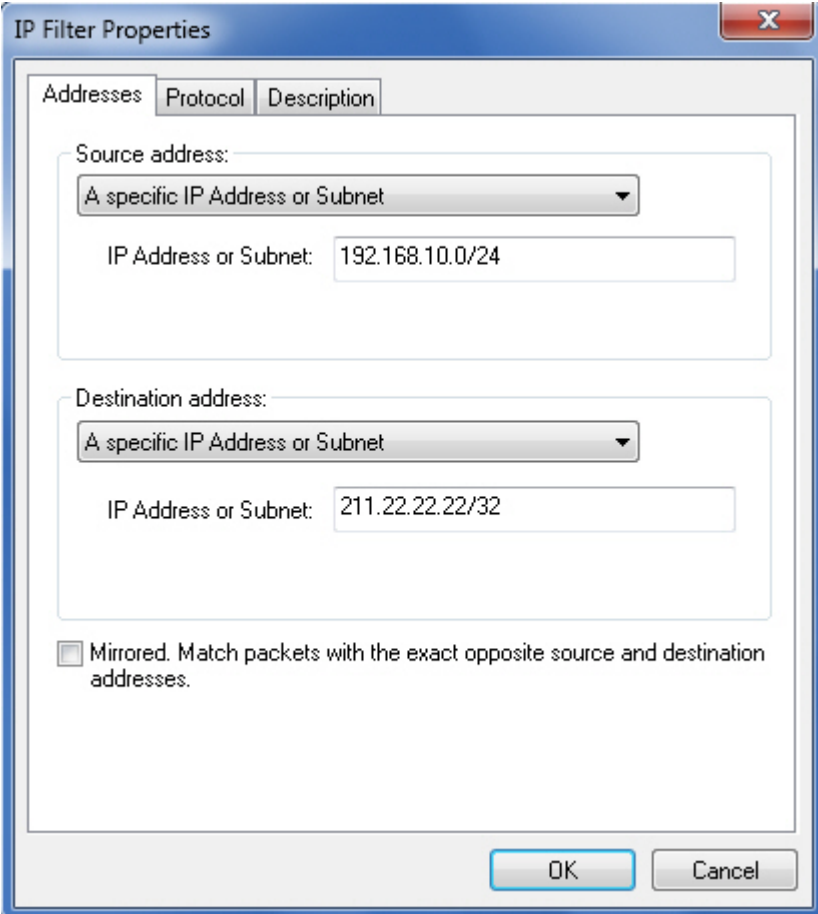




Adding an IP Filter List



Specifying a Name of the IP Filter List



The **IP Filter Properties** dialog box has three tabs: **Addresses**, **Protocol**, and **Description**. The **Addresses** tab is active.

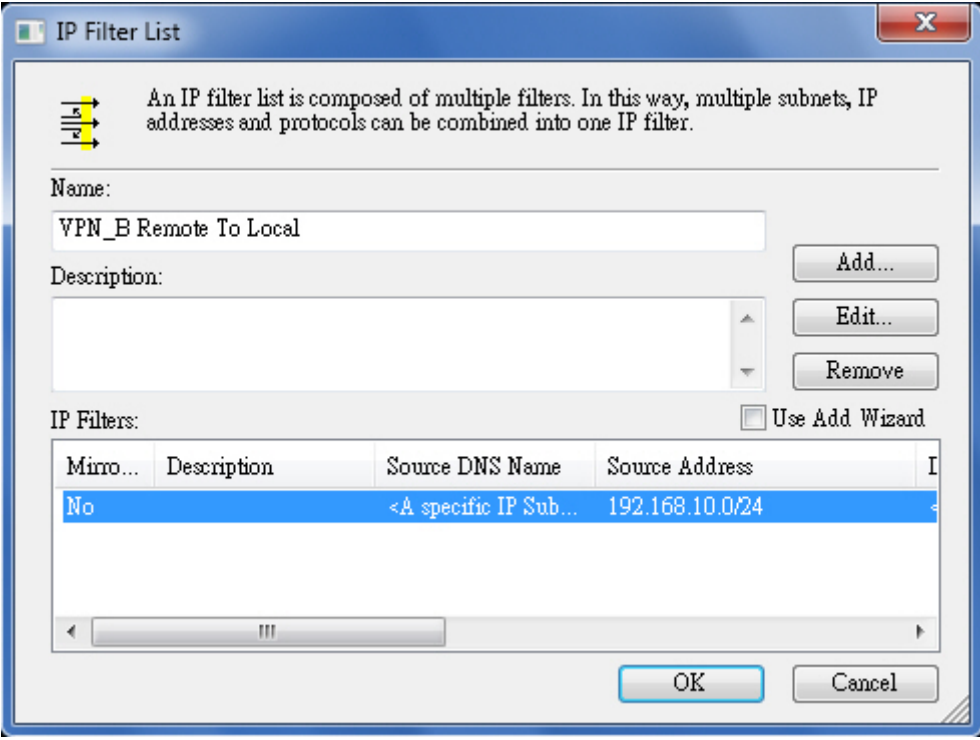
Source address:
A dropdown menu shows "A specific IP Address or Subnet". Below it, the **IP Address or Subnet** field contains "192.168.10.0/24".

Destination address:
A dropdown menu shows "A specific IP Address or Subnet". Below it, the **IP Address or Subnet** field contains "211.22.22.22/32".

☐ **Mirrored.** Match packets with the exact opposite source and destination addresses.

Buttons: **OK**, **Cancel**.

Specifying the Source and Destination Addresses



The **IP Filter List** dialog box contains an icon of three arrows and the text: "An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter."

Name:
VPN_B Remote To Local

Description:
[Empty text box]

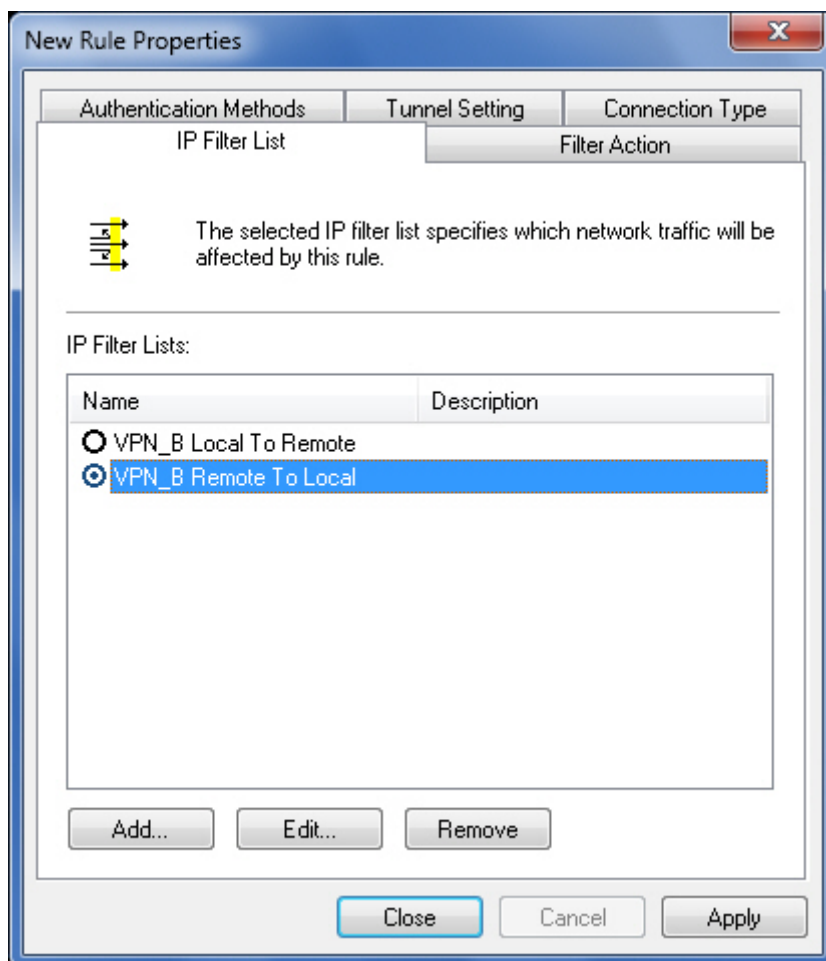
Buttons: **Add...**, **Edit...**, **Remove**.

IP Filters: ☐ Use Add Wizard

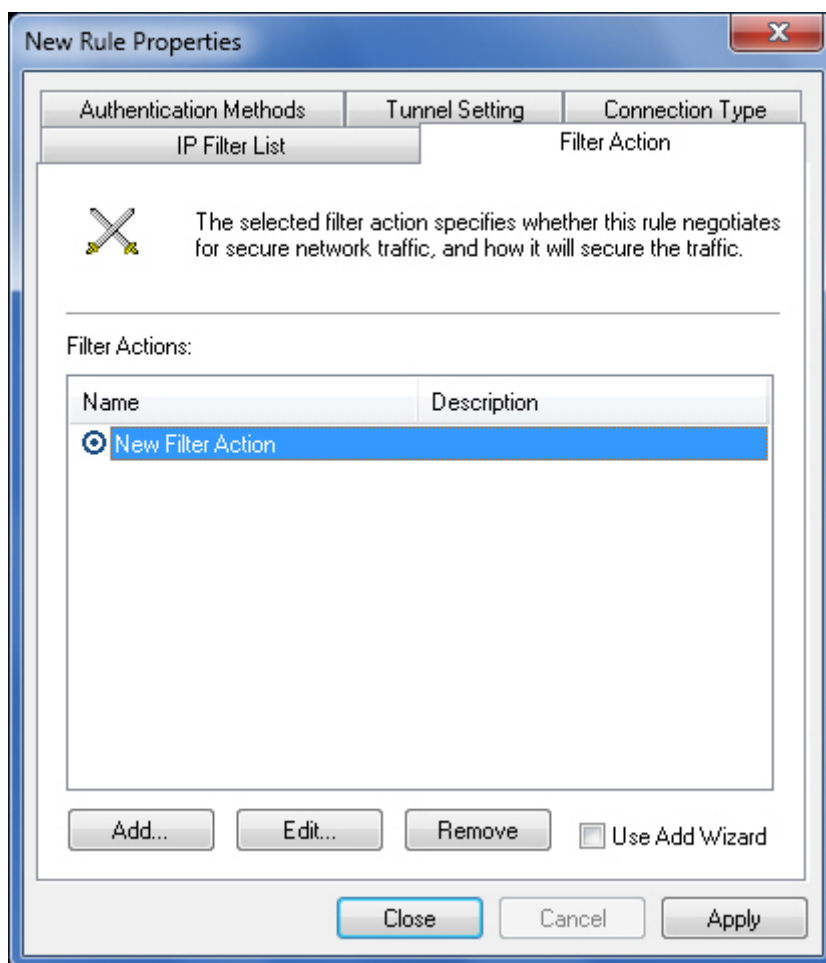
Mirro...	Description	Source DNS Name	Source Address
No	<A specific IP Sub...		192.168.10.0/24

Buttons: **OK**, **Cancel**.

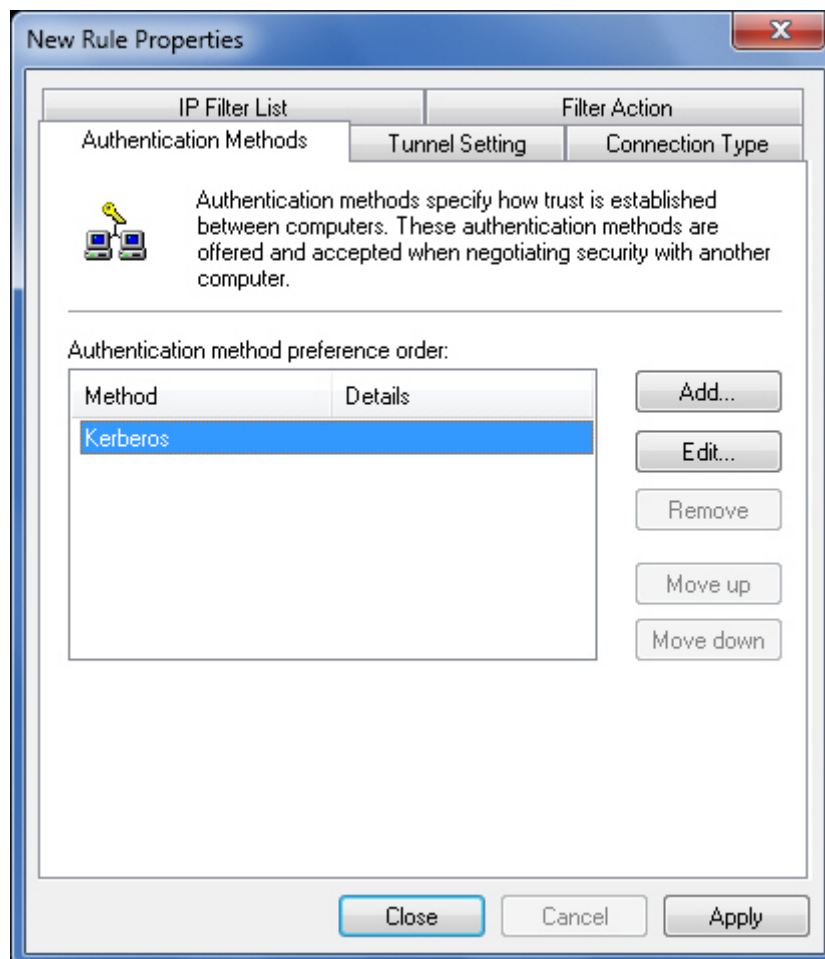
An IP Filter Successfully Added to the List



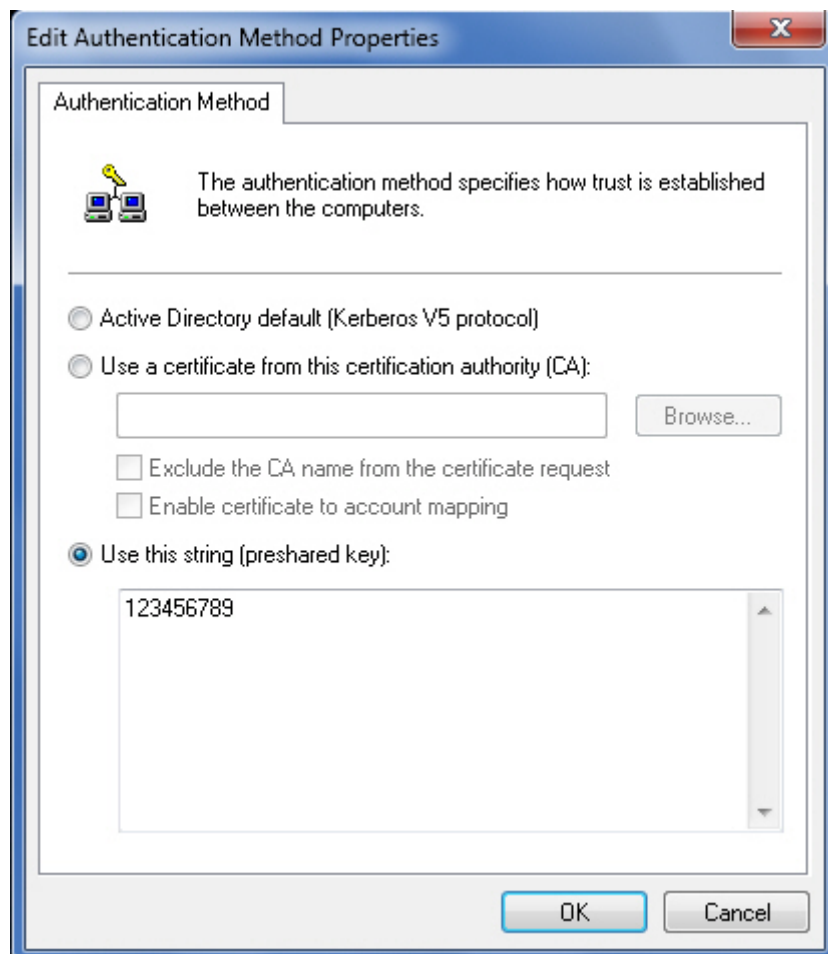
An IP Filter List Successfully Added to the Rule



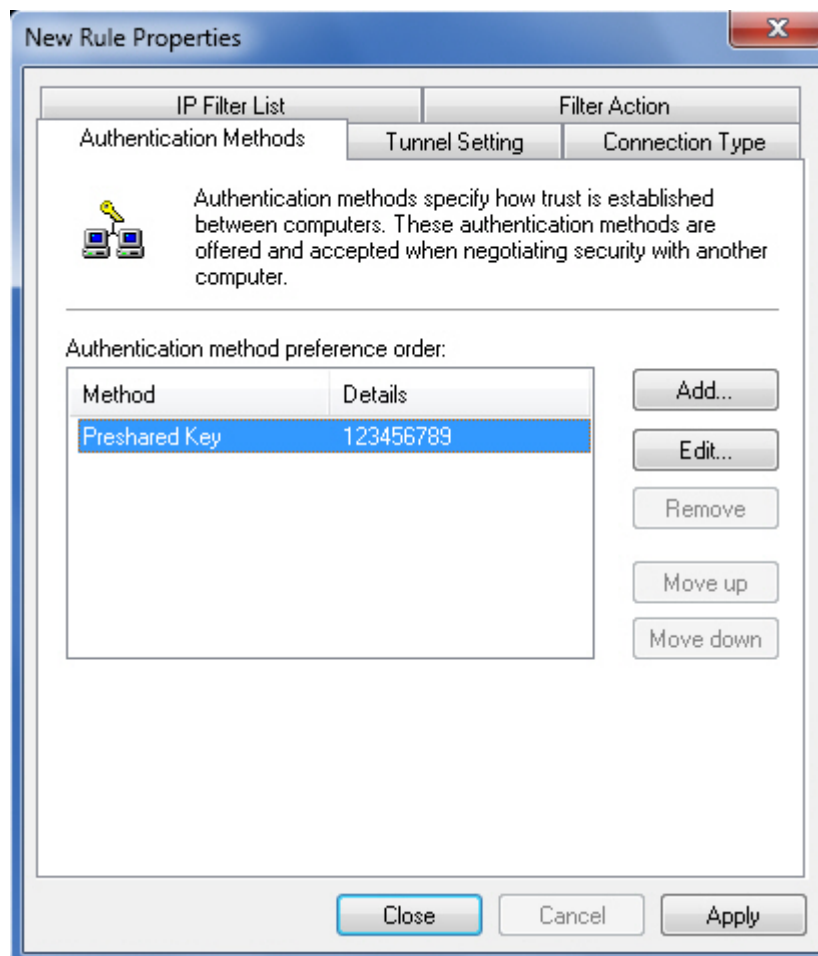
Adding a Filter Action



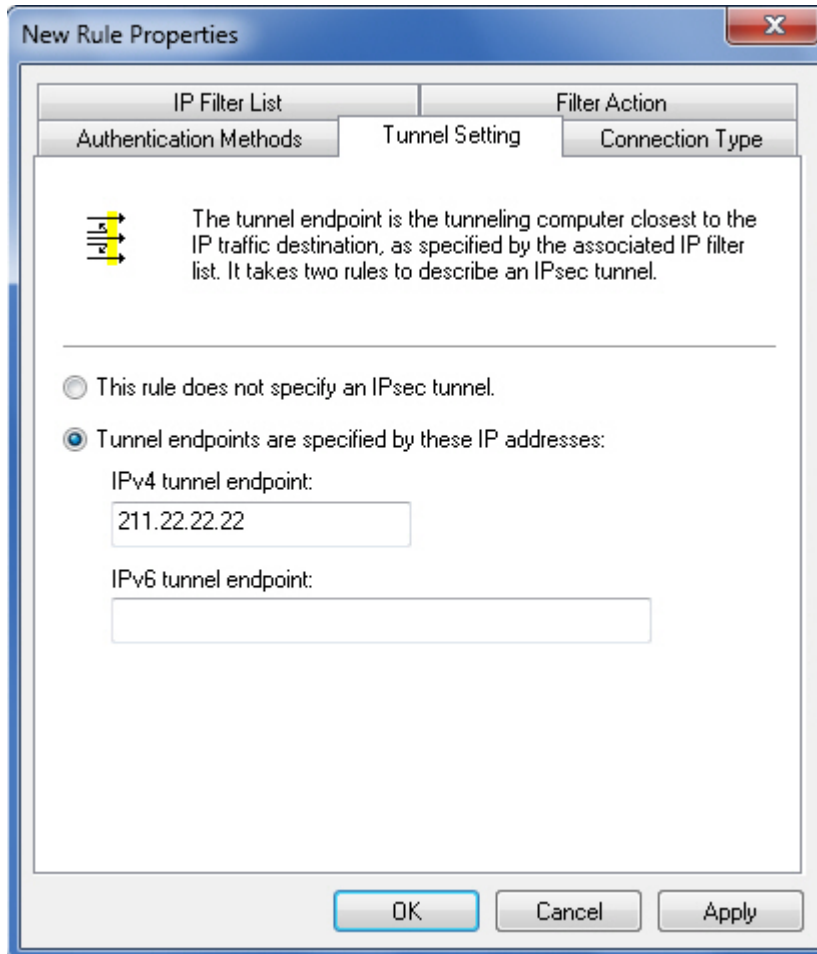
Editing the Authentication Method



Specifying a Preshared Key



Authentication Method Successfully Added to the Rule




The dialog box is titled "New Rule Properties" and has a close button (X) in the top right corner. It contains three tabs: "IP Filter List", "Filter Action", and "Authentication Methods". The "Filter Action" tab is selected, and it contains a "Tunnel Setting" sub-tab. The "Tunnel Setting" sub-tab is active, showing a description of tunnel endpoints and two radio button options. The first option is "This rule does not specify an IPsec tunnel." The second option is "Tunnel endpoints are specified by these IP addresses:", which is selected. Under this option, there are two text input fields: "IPv4 tunnel endpoint:" with the value "211.22.22.22" and "IPv6 tunnel endpoint:" which is empty. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

New Rule Properties

IP Filter List Filter Action

Authentication Methods Tunnel Setting Connection Type

 The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPsec tunnel.

☐ This rule does not specify an IPsec tunnel.

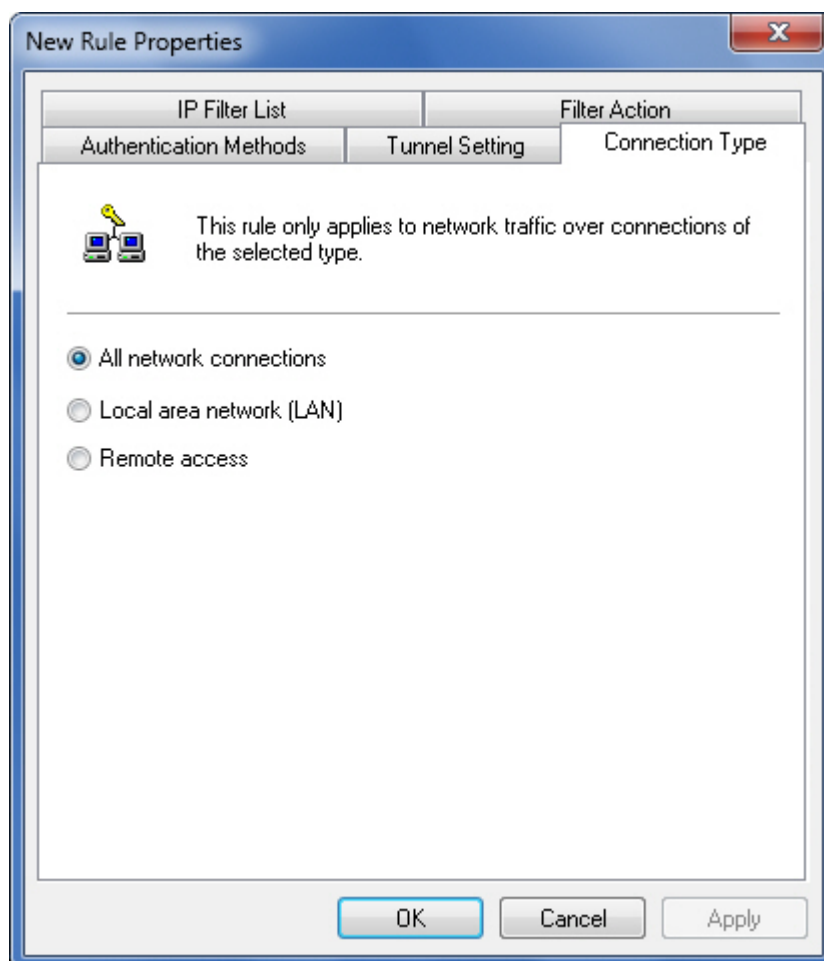
☒ Tunnel endpoints are specified by these IP addresses:

IPv4 tunnel endpoint:

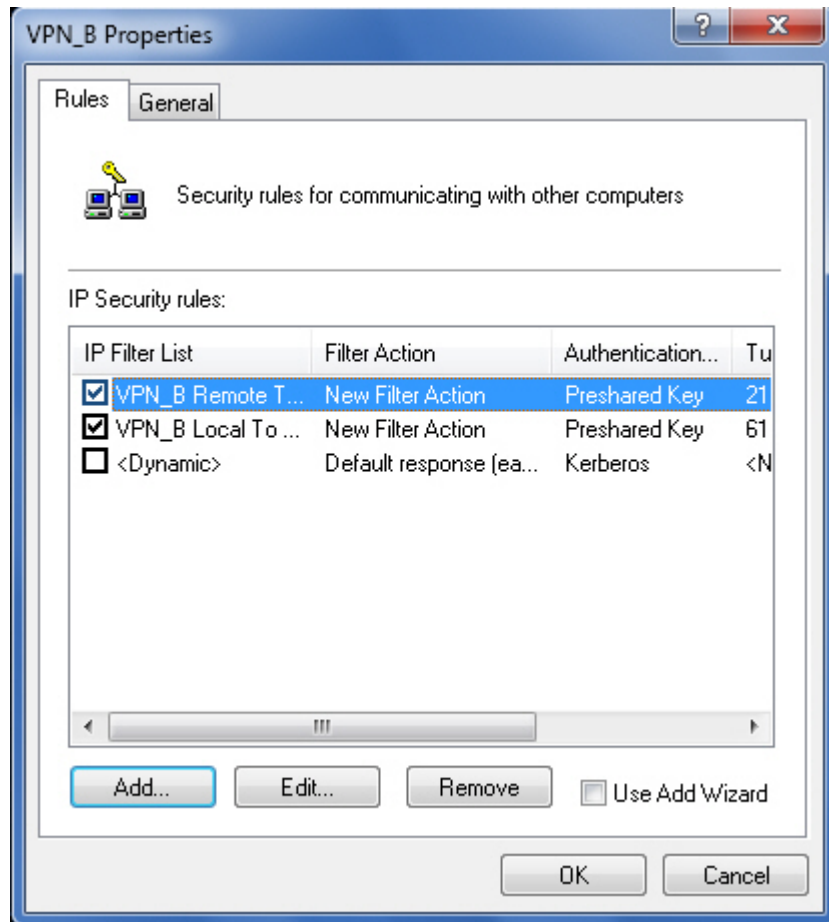
IPv6 tunnel endpoint:

OK Cancel Apply

Specifying the IPv4 Tunnel Endpoint



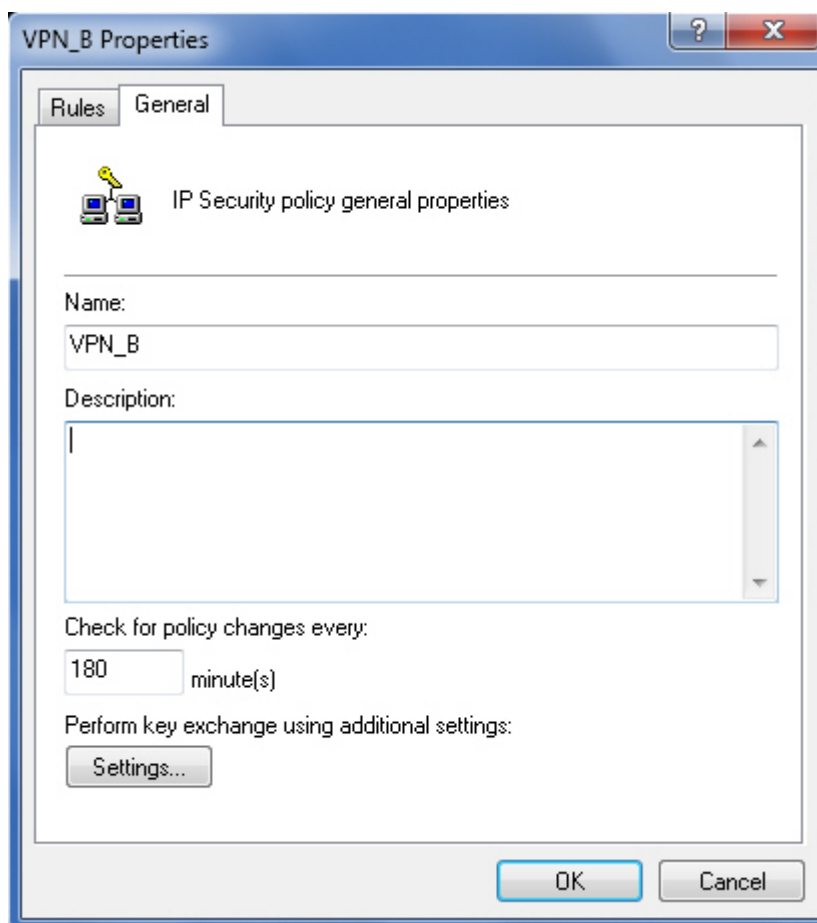
Applying the Rule to All Network Connections



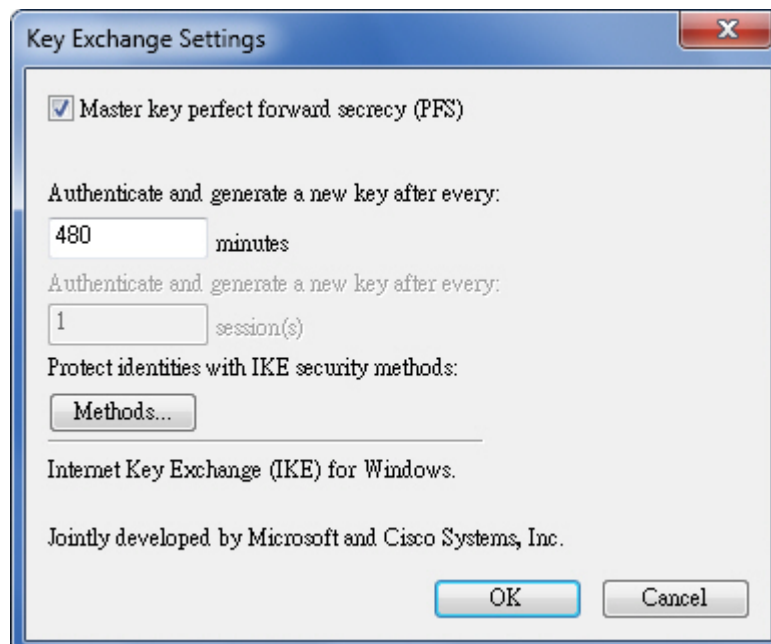
IP Security Rule Successfully Added

Step 4. In the **VPN_B Properties** dialog box, click the **General** tab and then set as shown below:

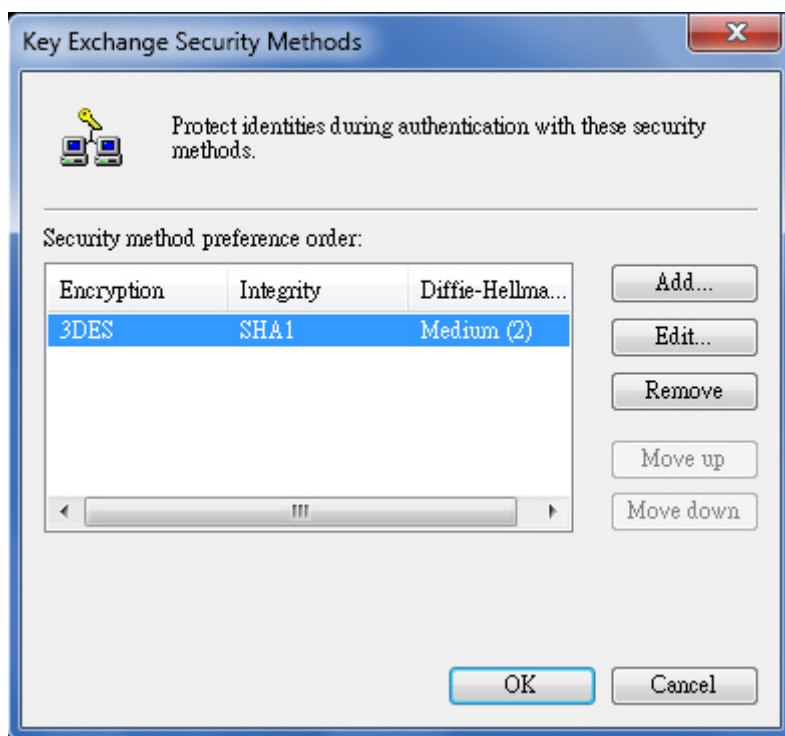
- Type in "VPN_B" in the **Name** field.
- Enter "180" in the minute(s) field.
- Click **Settings**.
- In the **Key Exchange Settings** dialog box, follow the steps below:
 - ◆ Tick the box of "Master key perfect forward secrecy (PFS)".
 - ◆ Enter "480" in the **minutes** field.
 - ◆ Click **Methods**.
 - ◆ In the **Key Exchange Security Methods** dialog box, select "3DES-SHA1-Medium(2)" from the **Security method preference order** and then click **Edit**.
 - In the **IKE Security Algorithms** dialog box, follow the steps below:
 - **Integrity algorithm:** Select "MD5".
 - **Encryption algorithm:** Select "3DES".
 - **Diffie-Hellman group:** Select "Medium (2)".
 - Click **OK**.
 - Click **OK**.
 - ◆ Click **OK**.
- Click **OK**.



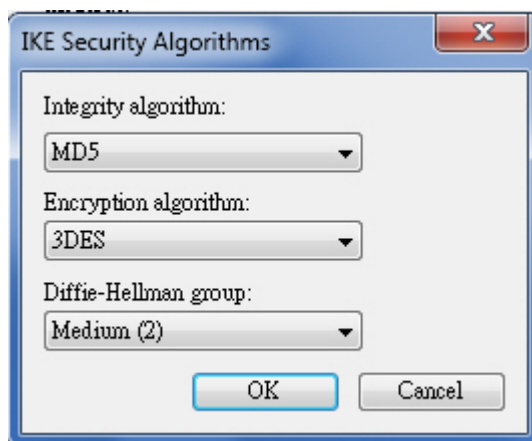
Configuring the IP Security Policy General Properties



Configuring the Key Exchange Settings



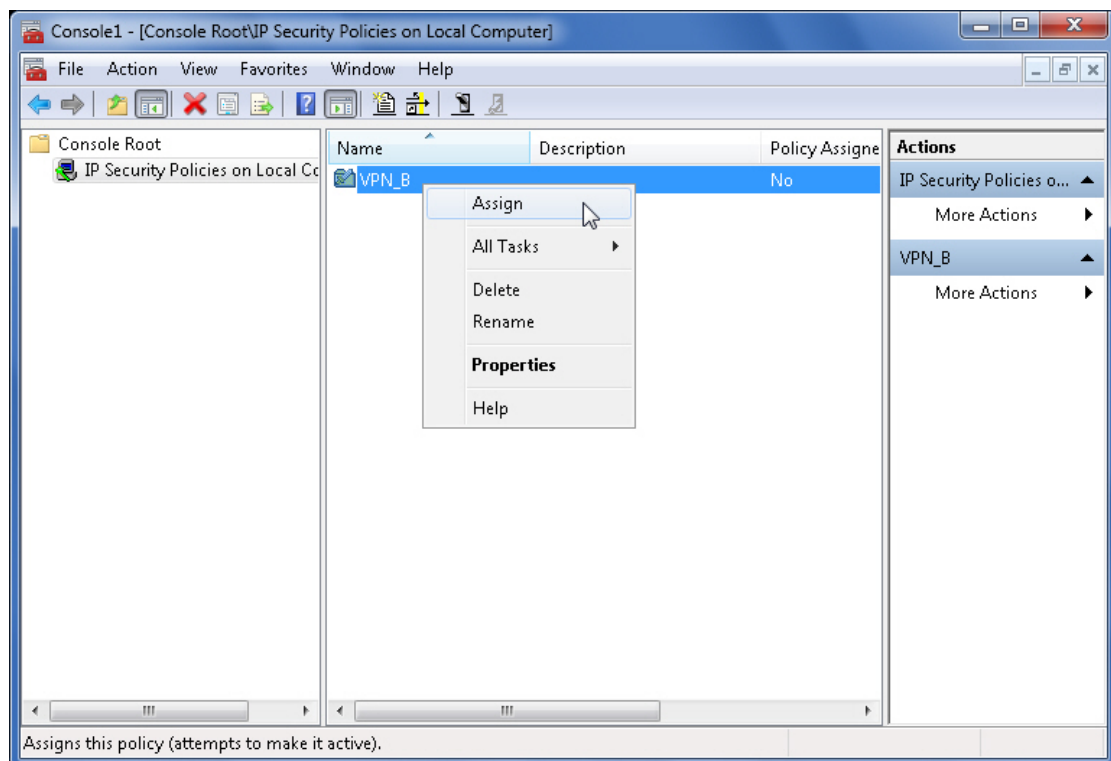
Configuring the Security Methods



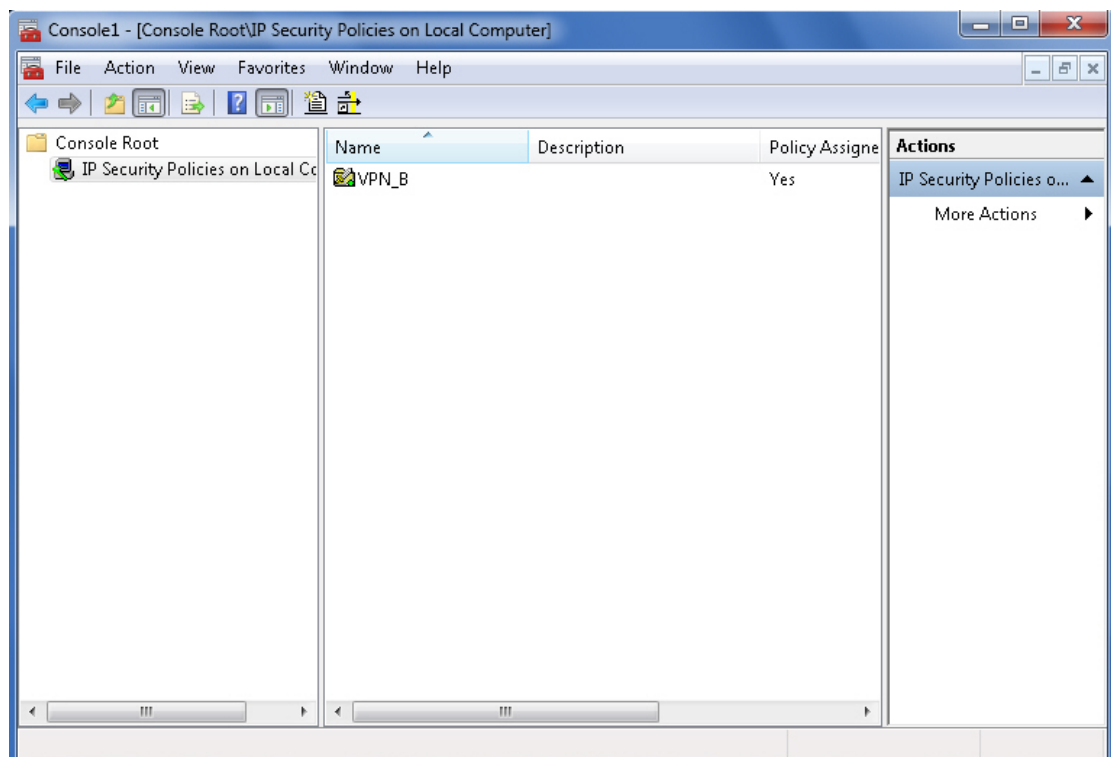
Customizing the IKE Security Algorithms

Step 5. In the **Microsoft Management Console** window, set as shown below:

- In the **Console Root** tree, click **IP Security Policies on Local Computer**, right-click the policy “VPN_B” and then select **Assign**.



Assigning an IP Security Policy



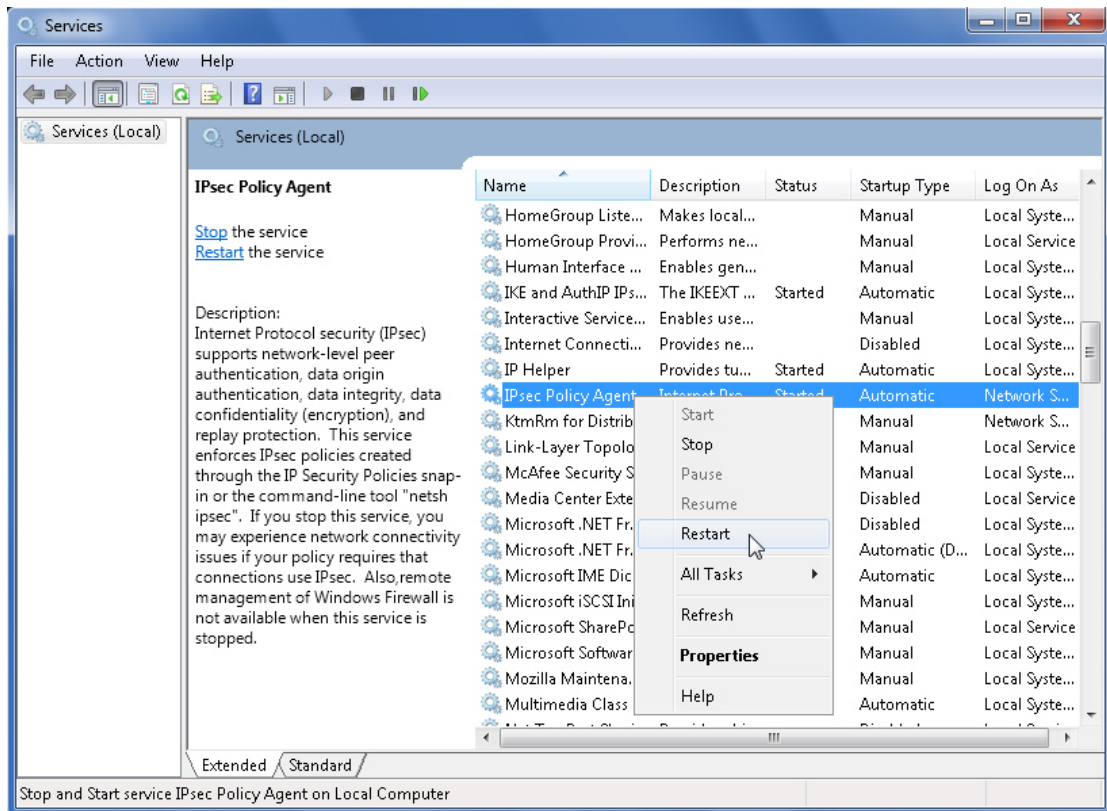
IP Security Policy Successfully Assigned

Step 6. Select **Services** on the **Start** menu or type in “services.msc” in the **Search** field, and then set as shown below:

- Scroll down to select **IPSec Policy Agent**, right-click it, and then select **Restart**.

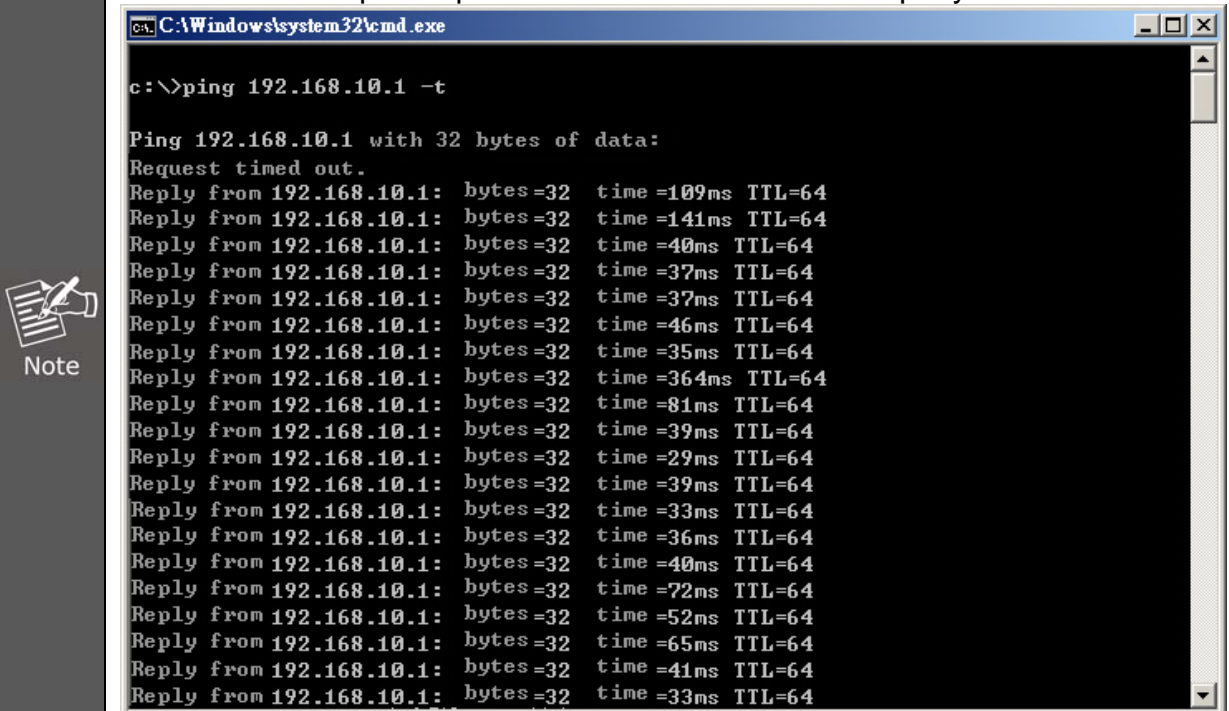


Selecting “Services” on the Start Menu

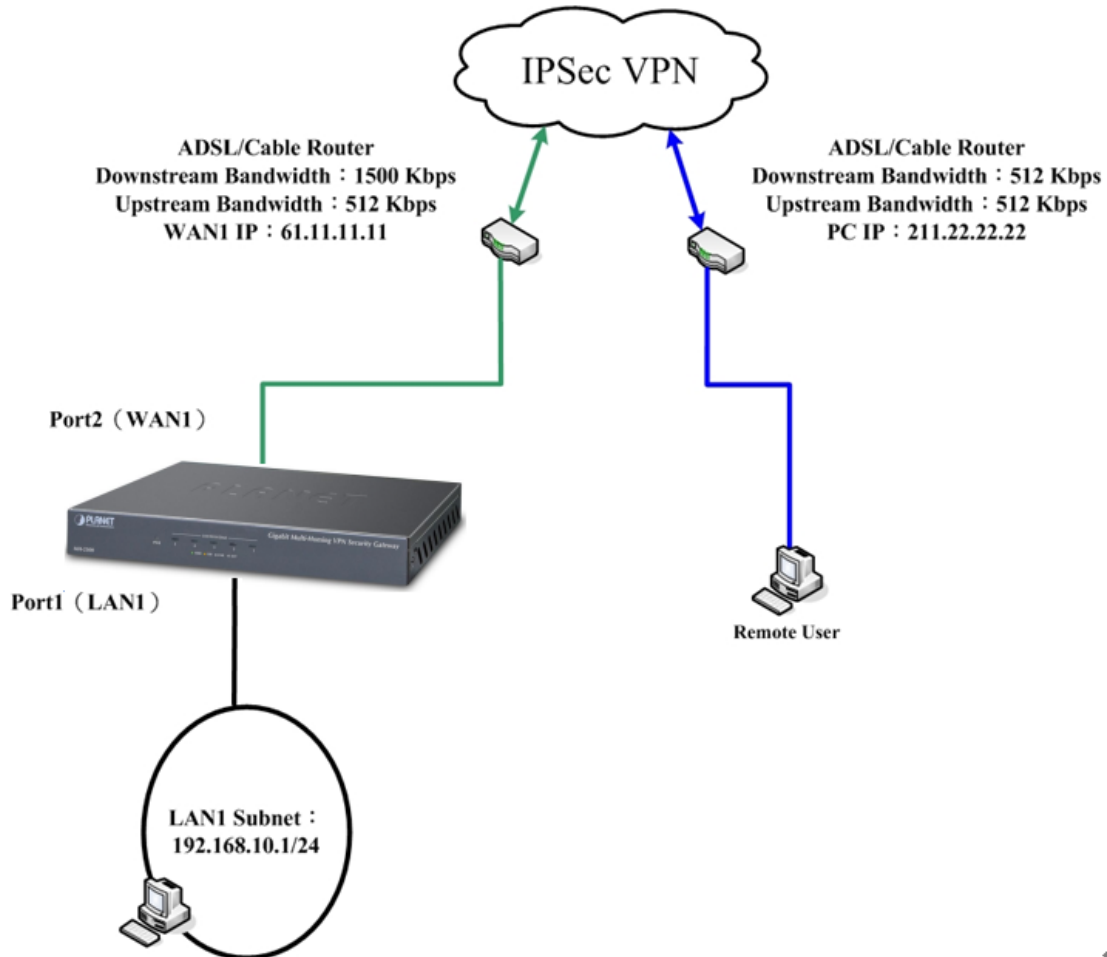


Restarting the IPsec Policy Agent

Once the configuration is completed, constantly ping the Company A's LAN subnet, such as 192.168.10.1. The IPsec VPN tunnel is only successfully established if response packets are received from Company A.



Step 7. IPSec VPN tunnel has been successfully established between the MH-2300 and the Windows 7 PC.



The Deployment of an IPSec VPN Network between MH-2300 and Windows7 PC

4.8.1.3 Using Two Units of MH-2300 to Establish an IPSec VPN Tunnel in Aggressive Mode

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Company A: Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Company B: Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x / 24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

This example will be using two units of MH-2300 to establish a VPN tunnel in Aggressive mode as follows:

For A Company, set as shown below:

Step 1. Go to **Policy Object > VPN > IPSec Autokey**, and then click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

[New Entry](#)

The IPSec Autokey Rule Table

Step 2. Enter “VPN_A” in the **Name** field and select “Port2 (WAN1)” for **Interface**.

Basic Settings (Required)	
Name :	<input type="text" value="ipsec1"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

Name and Interface Settings

Step 3. Select “Remote Gateway (Static IP or Hostname)” for **Remote Settings**, and enter the gateway address of B Company.

Remote Settings	
<input checked="" type="radio"/> Remote Gateway (Static IP or Hostname) :	<input type="text" value="211.22.22.22"/> (Max. 80 characters)
<input type="radio"/> Remote Gateway or Client (Dynamic IP)	

Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of the string is 62 characters).

Authentication Method :	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key String :	<input type="text" value="1234567890"/> (Max. 62 characters)

Authentication Method Settings

Step 5. In the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**; select “SHA1” for **Authentication Algorithm**, and then select “Diffie-Hellman 2” for **Key Group**.

Encryption and Data Integrity Algorithms Help	
ISAKMP Settings	
Encryption Algorithm :	<input type="text" value="3DES"/>
Authentication Algorithm :	<input type="text" value="SHA1"/>
Key Group :	<input type="text" value="Diffie-Hellman 2"/>

Encryption and Data Integrity Algorithms

Step 6. Tick the radio box of “Use both algorithms” in the **IPSec Settings** section, select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 7. In the **Advanced Settings (Optional)** section, select “DH 1” for **PFS Key Group**, enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field.



PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

Advanced Settings


Step 8. Select “Aggressive mode” for **IKE Negotiation** as well as enter “11.11.11.11” in the **Local ID** field and “@abc123” in the **Peer ID** field.



Local ID : 11.11.11.11 (Max. 80 characters)

Peer ID : @abc123 (Max. 80 characters)


IKE Negotiation Settings



The **Local ID / Peer ID** field can be:

- Left blank to use the public IP.
- Specified with a valid IP; the two fields cannot be identical, e.g., “11.11.11.11” and “22.22.22.22”.
- Specified with a leading at-sign (@) followed by an alphanumeric string, e.g., “@123a” or “@abcd1”.

Step 9. The IPSec autokey rule is successfully added.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	ipsec1	WAN1	211.22.22.22	3DES / MD5	—	Modify Remove



[New Entry](#)

IPSec Autokey Rule Successfully Added

Step 10. Under **Policy Object > VPN > Trunk**, set as shown below:

- **Name:** Specify a name for the VPN trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask of Company A.
- **Remote Settings:** Specify the subnet and netmask of Company B.
- Select “VPN_A” from the **Available Tunnels** column on the left, and the click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.

■ Click **OK**.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

-----Available Tunnels-----

Add >>

<< Remove

-----Applied Tunnels-----


ipsec1

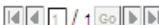
Keepalive IP Address :

☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

Adding a VPN Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	IPSec_vpn-tunnel	192.168.10.0 / 24	192.168.20.0 / 24	ipsec1	<input type="button" value="Modify"/> <input type="button" value="Remove"/>



VPN Trunk Successfully Added

Step 11. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk from the **VPN Trunk**.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼

Destination Address : Outside Any ▼

Service : Any ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : IPSec_vpn-tunnel ▼

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼

Application Blocking : ----- None ----- ▼

Advanced Settings

OK
Cancel

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any	VPN									Modify	Remove	Pause	1 ▼

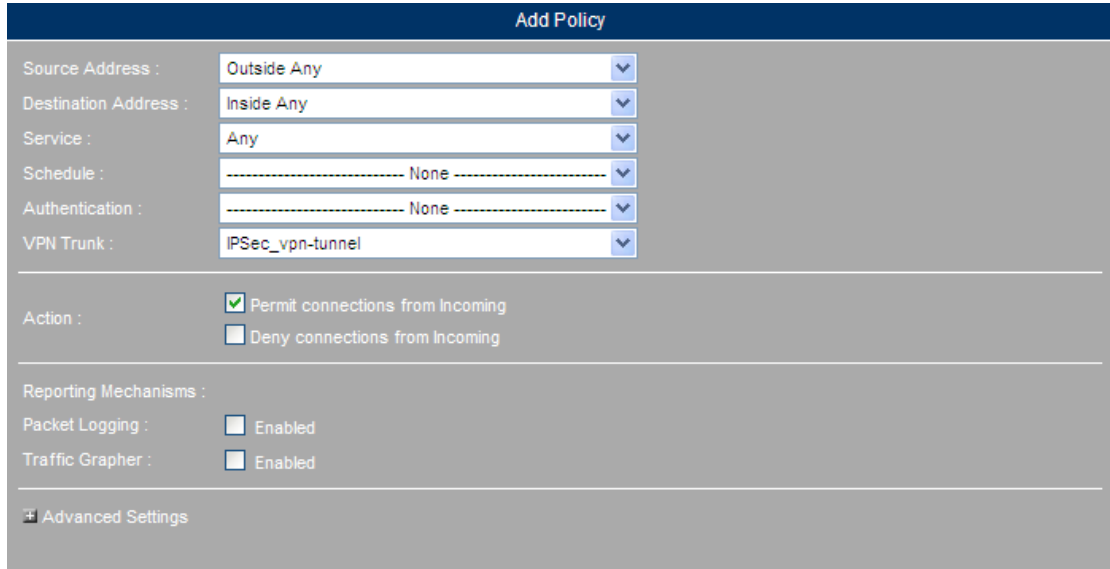
/ 1 Go

New Entry

Policy Successfully Created

Step 12. Under **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the defined trunk from the **VPN Trunk** drop-down list.
- Click **OK**.



Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

Policy Successfully Created

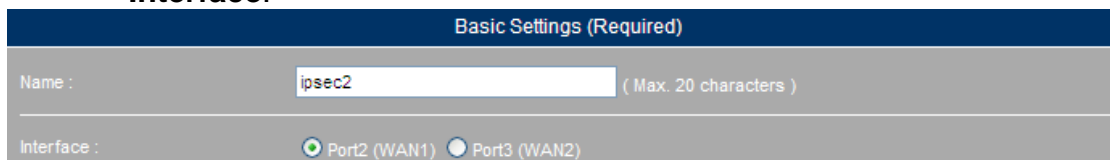
For B Company, set as shown below:

Step 1. Under **Policy Object > VPN > IPSec Autokey**, click **New Entry** and then set as shown below:

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

The IPSec Autokey Rule Table

Step 2. Enter "VPN_B" in the **Name** field and then select "Port2 (WAN1)" for **Interface**.



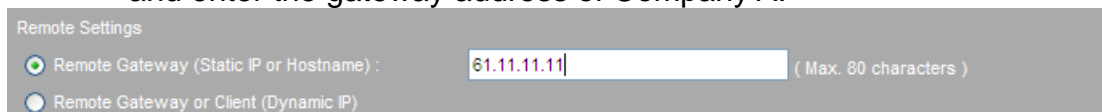
Basic Settings (Required)

Name : (Max. 20 characters)

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2)

Name and Interface Settings

Step 3. **Remote Settings:** Select “Remote Gateway (Static IP or Hostname)”, and enter the gateway address of Company A.




Remote Settings

☒ Remote Gateway (Static IP or Hostname) : 61.11.11.11 (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method**, and enter a **Pre-Shared Key String**. (The maximum length of the string is 62 characters)



Authentication Method : Pre-Shared Key

Pre-Shared Key String : 1234567890 (Max. 62 characters)

Authentication Method Settings

Step 5. In the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, select “SHA1” for **Authentication Algorithm**; and then select “Diffie-Hellman 2” for **Key Group**.



Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm : 3DES

Authentication Algorithm : SHA1

Key Group : Diffie-Hellman 2

Encryption and Data Integrity Algorithms

Step 6. Tick the radio box of “Use both algorithms” in the **IPSec Settings** section, select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

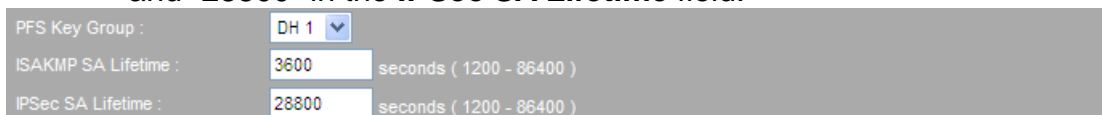
Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 7. In the **Advanced Settings (optional)** section, select “DH 1” for **PFS Key Group** as well as enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field.



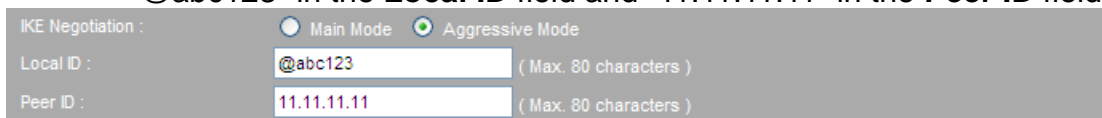
PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

Advanced Settings

Step 8. Select “Aggressive Mode” for **IKE Negotiation** as well as enter “@abc123” in the **Local ID** field and “11.11.11.11” in the **Peer ID** field.




IKE Negotiation : ☐ Main Mode ☒ Aggressive Mode

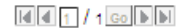
Local ID : @abc123 (Max. 80 characters)

Peer ID : 11.11.11.11 (Max. 80 characters)

IKE Negotiation Settings

Step 9. The IPSec autokey rule is successfully added.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	ipsec2	WAN1	61.11.11.11	3DES / MD5	—	Modify Remove



[New Entry](#)

IPSec Autokey Rule Successfully Added

Step 10. Under **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:

- **Name:** Specify a name for the VPN Trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask for Company B.
- **Remote Settings:** Specify the subnet and netmask of Company A.
- **Tunnel Selection:** Select “VPN_B” from the **Available Tunnels** column on the left, and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

Add >>

<< Remove

=====Applied Tunnels=====

ipsec2

Keepalive IP Address :


☒ Enable NetBIOS Broadcast over VPN

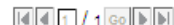
☐ Split task traffic across tunnels

[OK](#)

[Cancel](#)

Adding a VPN Trunk

Status	Name	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	IPSec_vpn-tunnel	192.168.20.0 / 24	192.168.10.0 / 24	ipsec2	Modify Remove



[New Entry](#)

VPN Trunk Successfully Added

Step 11. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK**.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

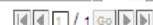
Application Blocking :

☐ Advanced Settings

[OK](#) [Cancel](#)

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1



[New Entry](#)

Policy Successfully Created

Step 12. Under **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address : Outside Any

Destination Address : Inside Any

Service : Any

Schedule : ----- None -----

Authentication : ----- None -----

VPN Trunk : IPSec_vpn-tunnel

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

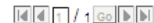
Traffic Grapher : ☐ Enabled

+ Advanced Settings

OK
Cancel

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1



New Entry

Policy Successfully Created

Step 13. IPSec VPN tunnel has been successfully established in Aggressive mode between two sites.

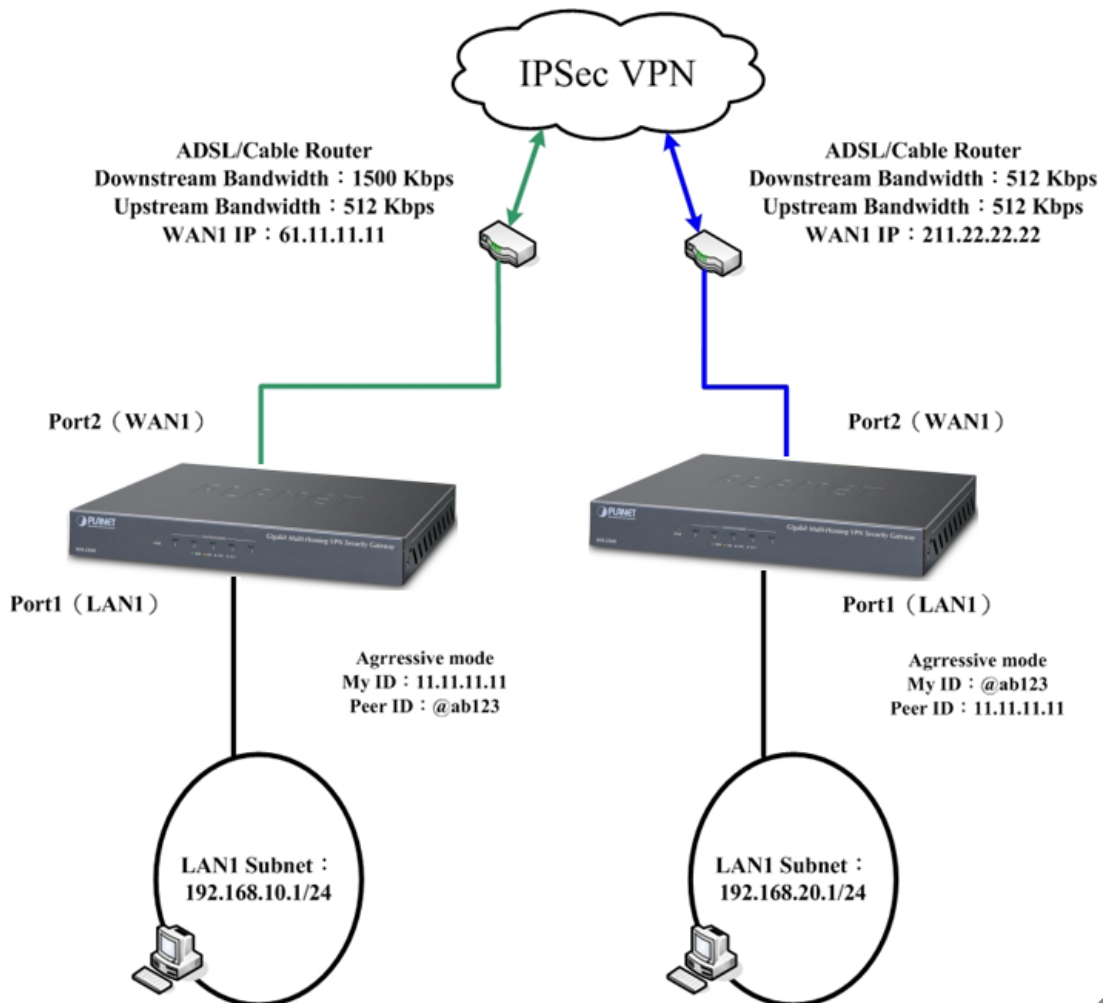


Figure 11-145 The Deployment of an IPSec VPN Network Running in Aggressive Mode between Two Units of MH-2300

4.8.1.4 Using Two Units of MH-2300 to Load Balance Outbound IPSec VPN Traffic with GRE Encapsulation

Prerequisite Configuration (Note: The IP Addresses are used as examples only)

[Company A]

Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x/24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Port 3 is defined as WAN 2 (61.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

[Company B]

Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x/24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

Port 3 is defined as WAN2 (211.33.33.33) and is connected to the Internet via the ADSL modem (ATUR).

Two IPsec VPN tunnels are established between Company A and B over their corresponding WAN 1 and WAN 2.

This example will be using two units of MH-2300 to establish two VPN tunnels with GRE encapsulation as follows:

For Company A, set as shown below:

Step 1. Under **Policy Object > VPN > IPsec Autokey**, click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

New Entry

The IPsec Autokey Rule Table

Step 2. Enter "VPN_01" in the **Name** field and then select "Port2 (WAN1)" for **Interface**.

Basic Settings (Required)	
Name :	VPN_01 (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

Name and Interface Settings

Step 3. **Remote Settings:** Select "Remote Gateway (Static IP or Hostname)", and specify the WAN1 gateway address of Company B.

Remote Settings	
<input checked="" type="radio"/> Remote Gateway (Static IP or Hostname) :	211.22.22.22 (Max. 80 characters)
<input type="radio"/> Remote Gateway or Client (Dynamic IP)	

Remote Settings

Step 4. Select "Pre-Shared Key" for **Authentication Method** and then type a key in the **Pre-Shared Key String** field, e.g., "123456789".

Authentication Method :	Pre-Shared Key ▼
Pre-Shared Key String :	123456789 (Max. 62 characters)

Authentication Method Settings

- Step 5. Under the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, “MD5” for **Authentication Algorithm** and “Diffie-Hellman1” for **Key Group**.



Encryption and Data Integrity Algorithms

- Step 6. Under the **IPSec Settings** section, select the radio box of “Use both algorithms”, select “3DES” for the **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.



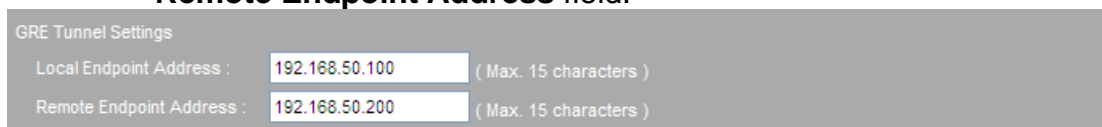
IPSec Algorithm Settings

- Step 7. Under the **Advanced Settings (optional)** section, select “DH1” for **PFS Key Group**, type “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field, and then select “Main Mode” for **IKE Negotiation**.

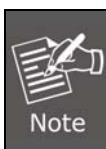


Advanced Settings

- Step 8. Under the **GRE Tunnel Settings** section, type in “192.168.50.100” in the **Local Endpoint Address** field and “192.168.50.200” in the **Remote Endpoint Address** field.




GRE Tunnel Settings



The **Local Endpoint Address** and **Remote Endpoint Address** must be in the same Class C subnet, and yet cannot be repeated.

Step 9. The IPSec autokey rule “VPN_01” is successfully added.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	—	Modify Remove

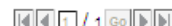


[New Entry](#)

IPSec Autokey Rule “VPN_01” Successfully Added

Step 10. Under **Policy Object > VPN > IPSec Autokey**, click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	—	Modify Remove



[New Entry](#)

The IPSec Autokey Rule Table

Step 11. Enter “VPN_02” in the **Name** field and select “Port3 (WAN2)” for **Interface**.

Basic Settings (Required)

Name : (Max. 20 characters)

Interface : ☐ Port2 (WAN1) ☒ Port3 (WAN2)

Name and Interface Settings

Step 12. **Remote Settings:** Select “Remote Gateway (Static IP or Hostname)” and enter the WAN 2 gateway address of Company B.

Remote Settings

☒ Remote Gateway (Static IP or Hostname) : (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

Configuring the Remote Settings

Step 13. Select “Pre-Shared Key” for **Authentication Method** and then type the same key as previously specified.

Authentication Method :

Pre-Shared Key String : (Max. 62 characters)

The Authentication Method Settings

Step 14. Under the **Encryption and Data Integrity Algorithms** section, select “3DES” for **Encryption Algorithm**, “MD5” for **Authentication Algorithm** and “Diffie-Hellman 1” for **Key Group**.

Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm :

Authentication Algorithm :

Key Group :

Encryption and Data Integrity Algorithms

Step 15. Under the **IPSec Settings** section, select the radio box of “Use both algorithms”, and then select “3DES” for **Encryption Algorithm** and

“MD5” for **Authentication Algorithm**.

IPSec Settings

☒ Use both algorithms

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 16. Under the **Advanced Settings (optional)** section, select “DH1” for **PFS Key Group**, enter “3600” in the **ISAKMP SA Lifetime** field, “28800” in the **IPSec SA Lifetime** field, and then select “Main Mode” for **IKE Negotiation**.

PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

The Advanced Settings

Step 17. Under the **GRE Tunnel Settings** section, type in “192.168.60.100” in the **Local Endpoint Address** field and “192.168.60.200” in the **Remote Endpoint Address** field.



GRE Tunnel Settings

Local Endpoint Address : 192.168.60.100 (Max. 15 characters)

Remote Endpoint Address : 192.168.60.200 (Max. 15 characters)

The GRE Tunnel Settings

Step 18. The IPSec autokey rule “VPN_02” is successfully added. ([Figure 11-163](#))

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	---	Modify Remove
	VPN_02	WAN2	211.33.33.33	3DES / MD5	---	Modify Remove

1 / 1 [Go](#)

[New Entry](#)

IPSec Autokey Rule “VPN_02” Successfully Added

Step 19. Under **Policy Object > VPN > Trunk**, set as shown below:

- **Name:** Specify a name for VPN Trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask of Company A.
- **Remote Settings:** Specify the subnet and netmask of Company B.
- Select “VPN_01” and “VPN_02” from the **Available Tunnels** column on the left, and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

Add >>

<< Remove

=====Applied Tunnels=====

VPN_01


VPN_02


Keepalive IP Address :

☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

Adding a VPN Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.10.0 / 24	192.168.20.0 / 24	VPN_01, VPN_02	<div style="display: flex; justify-content: space-between;"> Modify Remove </div>



New Entry

VPN Trunk Successfully Added

247

Step 20. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address : Inside Any ▼
Destination Address : Outside Any ▼
Service : Any ▼
Schedule : ----- None ----- ▼
Authentication : ----- None ----- ▼
VPN Trunk : ipsec-vpn-trunk ▼

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :
Packet Logging : ☐ Enabled
Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼
Application Blocking : ----- None ----- ▼

Advanced Settings

OK
Cancel

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any	VPN									Modify	Remove	Pause	1 ▼

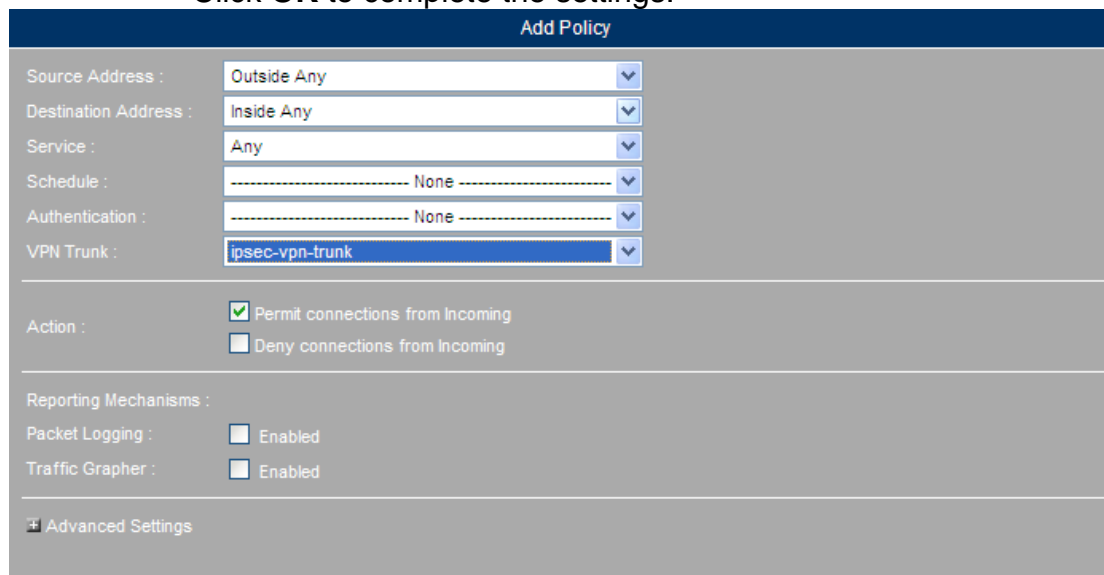
⏮ ⏪ ⏩ ⏭ / 1 Go ⏮ ⏪ ⏩ ⏭

New Entry

Policy Successfully Created

Step 21. Under **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.



OK Cancel

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1

1 / 1 Go

New Entry

Policy Successfully Created

For Company B, set as shown below:

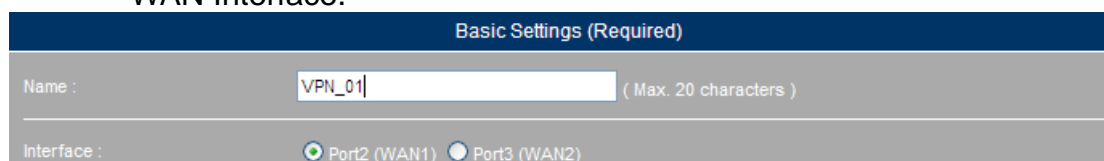
Step 1. Go to **Policy Object > VPN > IPSec Autokey**, and then click **New Entry**.

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

New Entry

IPSec Autokey Screen

Step 2. Type VPN_01 in the **Name** field and then select **Port2(WAN1)** for WAN Interface.



Name and WAN Interface Settings

Step 3. For **Remote Settings**, select **Remote Gateway (Static IP or Hostname)**, and enter the management address of A Company (WAN

pot 1).

Remote Settings

☒ Remote Gateway (Static IP or Hostname) : (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

Remote Settings

Step 4. Select “Pre-Shared Key” for **Authentication Method** and enter the **Pre-Shared Key String**.

Authentication Method :

Pre-Shared Key String : (Max. 62 characters)

IPSec Algorithm Settings

Step 5. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.

Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm :

Authentication Algorithm :

Key Group :

ISAKMP Algorithm Settings

Step 6. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.

IPSec Settings

☒ Use both algorithms

Encryption Algorithm :

Authentication Algorithm :

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 7. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.

PFS Key Group :

ISAKMP SA Lifetime : seconds (1200 - 86400)

IPSec SA Lifetime : seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

Advanced Settings of IPSec Autokey

Step 8. For **GRE Tunnel Settings**, type “192.168.50.200” in the **Local Endpoint Address** field and “192.168.50.100” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)


GRE Tunnel Settings

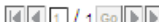
Local Endpoint Address : (Max. 15 characters)

Remote Endpoint Address : (Max. 15 characters)

GRE Tunnel Settings

Step 9. Settings completed.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	61.11.11.11	3DES / MD5	—	Modify Remove



[New Entry](#)

IPSec Autokey Settings Completed

Step 10. Under **Policy Object > VPN > IPSec Autokey**, click **New Entry** again.

Step 11. Type VPN_02 in the **Name** field and then select Port3 (WAN2) for **Interface**.

Basic Settings (Required)

Name : (Max. 20 characters)

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2)

Name and Interface Settings

Step 12. Select **Remote Gateway (Static IP or Hostname)** for **Remote Settings**, and enter the management address of A Company (WAN port 2).

Remote Settings

☒ Remote Gateway (Static IP or Hostname) : (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

Remote Settings

Step 13. Select “Pre-Shared Key” for **Authentication Method** and enter the **Pre-Shared Key String**.

Authentication Method :

Pre-Shared Key String : (Max. 62 characters)

Authentication Method Settings

Step 14. Below **Encryption and Data Integrity Algorithms**, select “3DES” for **Encryption Algorithm**; select “MD5” for **Authentication Algorithm**; select “DH 1” for **Key Group**.



Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm : 3DES

Authentication Algorithm : MD5

Key Group : Diffie-Hellman 1

ISAKMP Algorithm Settings

Step 15. Select **Use both algorithms** below the **IPSec Algorithm**, or tick **Use authentication algorithm only**. If ticked **Use both algorithms**, please select “3DES” for **Encryption Algorithm** and “MD5” for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

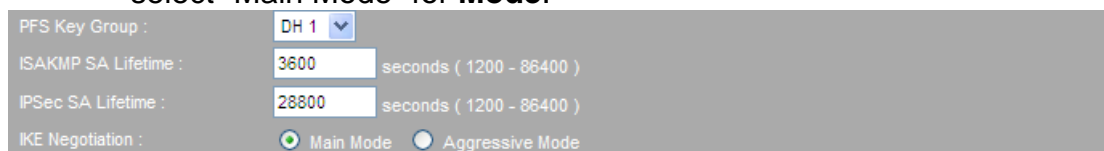
Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

IPSec Algorithm Settings

Step 16. Select “Group 1” for **PFS Key Group**. Enter “3600” in the **ISAKMP SA Lifetime** field and “28800” in the **IPSec SA Lifetime** field and then select “Main Mode” for **Mode**.



PFS Key Group : DH 1

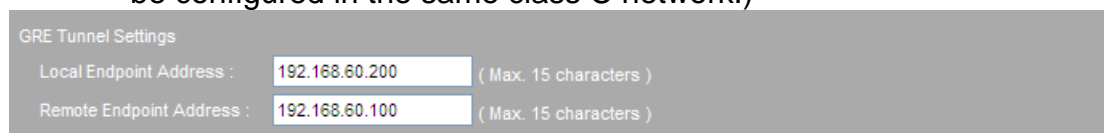
ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

Advanced Settings of IPSec Autokey

Step 17. For **GRE Tunnel Settings**, type “192.168.60.200” in the **Local Endpoint Address** field and “192.168.60.100” in the **Remote Endpoint Address** field. (Note: The local IP and the remote IP must be configured in the same class C network.)





GRE Tunnel Settings

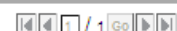
Local Endpoint Address : 192.168.60.200 (Max. 15 characters)

Remote Endpoint Address : 192.168.60.100 (Max. 15 characters)

GRE Tunnel Settings

Step 18. Settings completed.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	61.11.11.11	3DES / MD5	---	Modify Remove
	VPN_02	WAN1	61.22.22.22	3DES / MD5	---	Modify Remove

 / 1 Go

[New Entry](#)

IPSec Autokey Settings Completed

- Step 19. Under **Policy Object > VPN > Trunk**, set as shown below:
- **Name:** Type a name.
 - **Local Settings:** Select "LAN". **Local IP / Netmask:** Type "192.168.20.0" as B Company's subnet address and "255.255.255.0" as **Mask**.
 - **Remote Settings:** Select **Remote IP / Netmask**. **Remote IP / Netmask:** Type "192.168.10.0" as A Company's subnet address and "255.255.255.0" as **Mask**.
 - **Tunnel:** Select "VPN_01" and "VPN_02" and then add them to the right column.
 - Tick **Enable NetBIOS Broadcast over VPN**.
 - Click **OK**.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

Add >>

<< Remove

=====Applied Tunnels=====

VPN_01


VPN_02

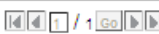
Keepalive IP Address :

☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

VPN Trunk Settings

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.20.0 / 24	192.168.10.0 / 24	VPN_01, VPN_02	<input type="button" value="Modify"/> <input type="button" value="Remove"/>



VPN Trunk Created

Step 20. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the defined trunk for **VPN Trunk**.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼
Destination Address : Outside Any ▼
Service : Any ▼
Schedule : ----- None ----- ▼
Authentication : ----- None ----- ▼
VPN Trunk : ipsec-vpn-trunk ▼

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :
Packet Logging : ☐ Enabled
Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼
Application Blocking : ----- None ----- ▼

Advanced Settings

OK

Cancel

Using VPN Trunk in an Outgoing Policy

Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any	VPN									Modify	Remove	Pause	1 ▼

New Entry

An Outgoing Policy with VPN Trunk

Step 21. Select **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the defined trunk for **VPN Trunk**.
- Click **OK**.

Add Policy

Source Address :

Outside Any

Destination Address :

Inside Any

Service :

Any

Schedule :

----- None -----

Authentication :

----- None -----

VPN Trunk :

ipsec-vpn-trunk

Action :

☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging :
☐ Enabled

Traffic Grapher :
☐ Enabled

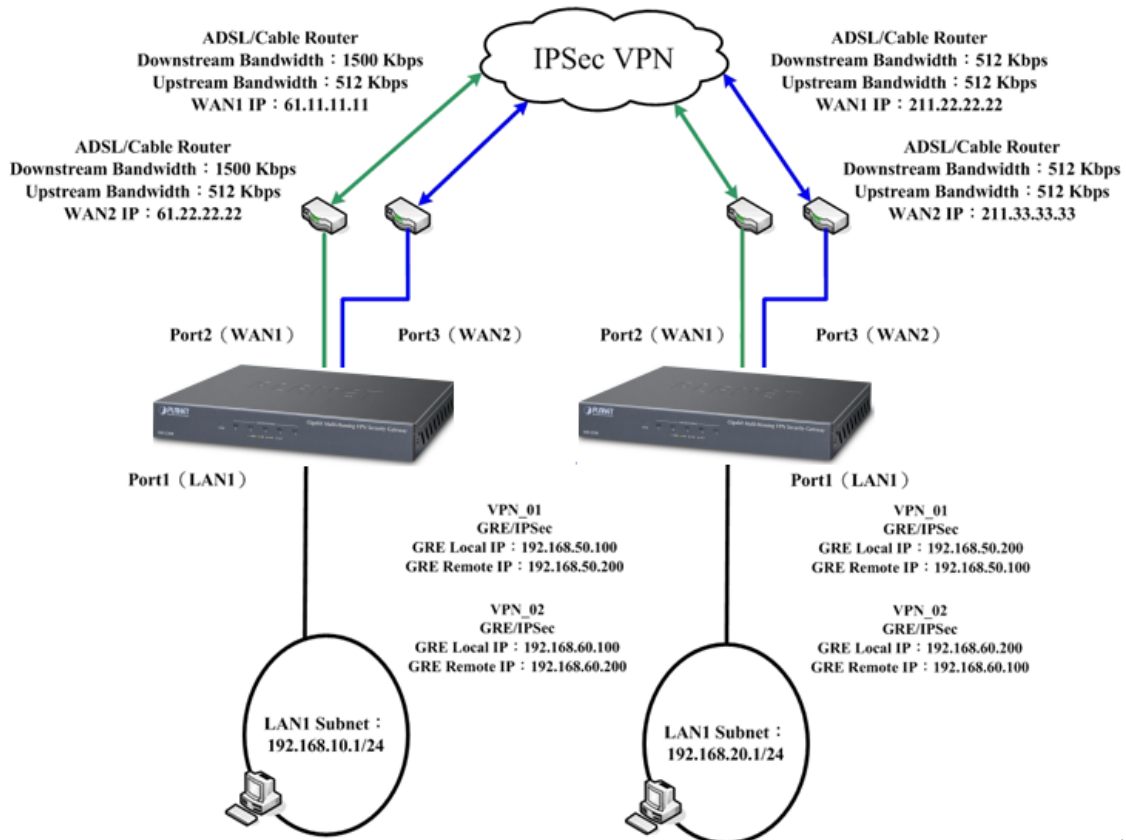
⚙️ Advanced Settings

Using VPN Trunk in an Incoming Policy

Source	Destination	Service	Action	Options					Configuration			Priority
Outside Any	Inside Any	Any	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	1

An Incoming Policy with VPN Trunk

Step 22. Settings completed.



Deployment of IPsec VPN Using GRE/IPsec

4.8.1.5 Using Three Units of MH-2300 to Create a Hub-and-Spoke IPsec VPN Network

Prerequisite Configuration (Note: The IP addresses are used as examples only)

[Company A]

Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

[Company B]

Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x / 24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

[Company C]

Port 1 is defined as LAN 1 (192.168.30.1) and is connected to the LAN subnet 192.168.30.x / 24.

Port 2 is defined as WAN 1 (121.33.33.33) and is connected to the Internet via the ADSL modem (ATUR).

This example will be using three units of MH-2300 to create a hub-and-spoke IPSec VPN network as follows:

For Company A, set as shown below:

Step1. Go to **Policy Object > VPN > IPSec Autokey** and then click **New Entry**.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

[New Entry](#)
[IPSec Autokey](#)

Step2. Type VPN_01 in the **Name** field and then select Port2 (WAN1) for **Interface**.

Basic Settings (Required)	
Name :	<input type="text" value="VPN_01"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

[Configuring the Name and the Interface](#)

Step3. Under the **Remote Settings** section, select the **Remote Gateway (Static IP or Hostname)** and then fill out the blank.

Remote Settings	
<input checked="" type="radio"/> Remote Gateway (Static IP or Hostname) :	<input type="text" value="211.22.22.22"/> (Max. 80 characters)
<input type="radio"/> Remote Gateway or Client (Dynamic IP)	

[Configuring the Static IP or Hostname](#)

Step4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.

Authentication Method :	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key String :	<input type="text" value="123456789"/> (Max. 62 characters)

[Configuring the Authentication Method](#)

Step5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH 1 for **Key Group**.



Configuring the IPsec Algorithm

Step6. Under the **IPsec Algorithm** section, select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.




Configuring the IPsec Algorithm

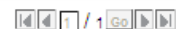
Step7. Under the **Advanced Settings (optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPsec SA Lifetime** field and then select Main mode for **Mode**.



Configuring the PFS Key Group, ISAKMP SA Lifetime, IPsec SA Lifetime and Mode

Step8. Policy Created.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	—	Modify Remove



[New Entry](#)
Policy Created

Step9. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:

- Type the name in the **Name** field.
- **Local Settings**: select LAN. Enter the local subnet and the mask.
- Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the local subnet and the mask.
- Move the VPN_01 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :
 Interface: ☒ LAN ☐ DMZ
 Local IP Address / Netmask : /

Remote Settings:
☒ Remote IP Address / Netmask : /
☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

Add >>

<< Remove

=====Applied Tunnels=====


VPN_01

Keepalive IP Address :
☒ Enable NetBIOS Broadcast over VPN
☐ Split task traffic across tunnels

OK

Cancel

Configuring the First Trunk


Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	vpn-trunk1	192.168.0.0 / 24	192.168.20.0 / 24	VPN_01	<div style="background-color: #90EE90; padding: 2px 5px;">Modify</div> <div style="background-color: #FFD700; padding: 2px 5px;">Remove</div>

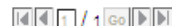
1 / 1 Go

New Entry

First Trunk Completed

Step10. Go to **Policy Object > VPN > IPSec Autokey** and then click the **New Entry** button again.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	—	Modify



[New Entry](#)

The IPSec Autokey Page

Step11. Type VPN_02 in the **Name** field and then select Port2(WAN1) for the **Interface**.

Basic Settings (Required)	
Name :	<input type="text" value="VPN_02"/> (Max. 20 characters)
Interface :	<input checked="" type="radio"/> Port2 (WAN1) <input type="radio"/> Port3 (WAN2)

Configuring the Name and the Interface

Step12. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then fill the field.

Remote Settings	
<input checked="" type="radio"/> Remote Gateway (Static IP or Hostname) :	<input type="text" value="121.33.33.33"/> (Max. 80 characters)
<input type="radio"/> Remote Gateway or Client (Dynamic IP)	

Configuring the Remote Gateway –Fixed IP or Domain Name

Step13. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.

Authentication Method :	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key String :	<input type="text" value="123456789"/> (Max. 62 characters)

Configuring the Authentication Method

Step14. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH 1 for **Key Group**.

Encryption and Data Integrity Algorithms Help	
ISAKMP Settings	
Encryption Algorithm :	<input type="text" value="3DES"/>
Authentication Algorithm :	<input type="text" value="MD5"/>
Key Group :	<input type="text" value="Diffie-Hellman 1"/>

Configuring ISAKMP Algorithm

Step15. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and MD5 for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

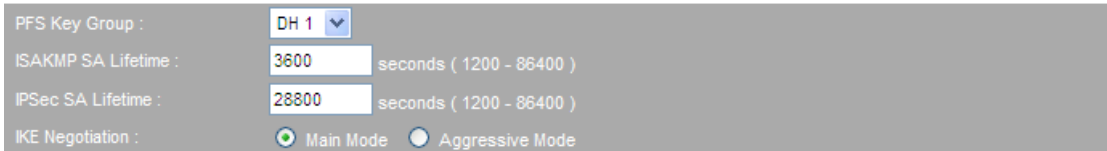
Encryption Algorithm : 3DES

Authentication Algorithm : MD5

☐ Use authentication algorithm only

Configuring IPSec Algorithm

Step16. Under the **Advanced Settings (optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPSec SA Lifetime** field and then select Main mode for **Mode**.



PFS Key Group : DH 1

ISAKMP SA Lifetime : 3600 seconds (1200 - 86400)

IPSec SA Lifetime : 28800 seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step17. Policy created.

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	211.22.22.22	3DES / MD5	---	Modify
	VPN_02	WAN1	121.33.33.33	3DES / MD5	---	Modify Remove

1 / 1 Go

[New Entry](#)
Policy Created

- Step18. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:
- Type the name in the **Name** field.
 - **Local Settings**: select LAN. Enter the IP address and the Mask in the **Local IP / Netmask** field.
 - Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the subnet and the mask.
 - Move the **VPN_02** from the **Available Tunnels** to the **Selected Tunnels**.
 - Tick **Enable NetBIOS Broadcast over VPN**.
 - Click **OK**.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

VPN_01

=====Applied Tunnels=====



VPN_02

Keepalive IP Address :

☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

Configuring the Second Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration	
	vpn-trunk1	192.168.0.0 / 24	192.168.20.0 / 24	VPN_01	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>
	vpn-trunk2	192.168.0.0 / 24	192.168.30.0 / 24	VPN_02	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

Total entries : 2

The Second Trunk Created


Step19. Go to **Policy Object > VPN > Trunk Group**, click **New Entry** and then set as shown below:

- Type the name in the **Name** field.
- Move the IPSec_VPN_Trunk_01(LAN) and IPSec_VPN_Trunk_02(LAN) from the **Available Trunks** column to the **Selected Trunks** column.
- Click **OK**.

Configuring the Trunk Group

Group Name ▲	Group Items	Configuration
vpn-trunk-group	vpn-trunk1, vpn-trunk2	Modify Remove

[New Entry](#)
Trunk Group Created


Note

The “IPSec_VPN_Trunk_01” (the VPN tunnel to Company A) and “IPSec_VPN_Trunk_02” (the VPN tunnel to Company B) under **Policy Object > VPN > Trunk** are mandatory for this hub-and-spoke IPSec VPN network.

Step20. Under **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼

Destination Address : Outside Any ▼

Service : Any ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : vpn-trunk-group ▼

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled
 Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼
 Application Blocking : ----- None ----- ▼

⚙️ Advanced Settings

OK
Cancel

Configuring the Outgoing Policy with VPN Trunk

Source	Destination	Service	Action	Options								Configuration			Priority
Inside Any	Outside Any	Any	VPN									Modify	Remove	Pause	1 ▼

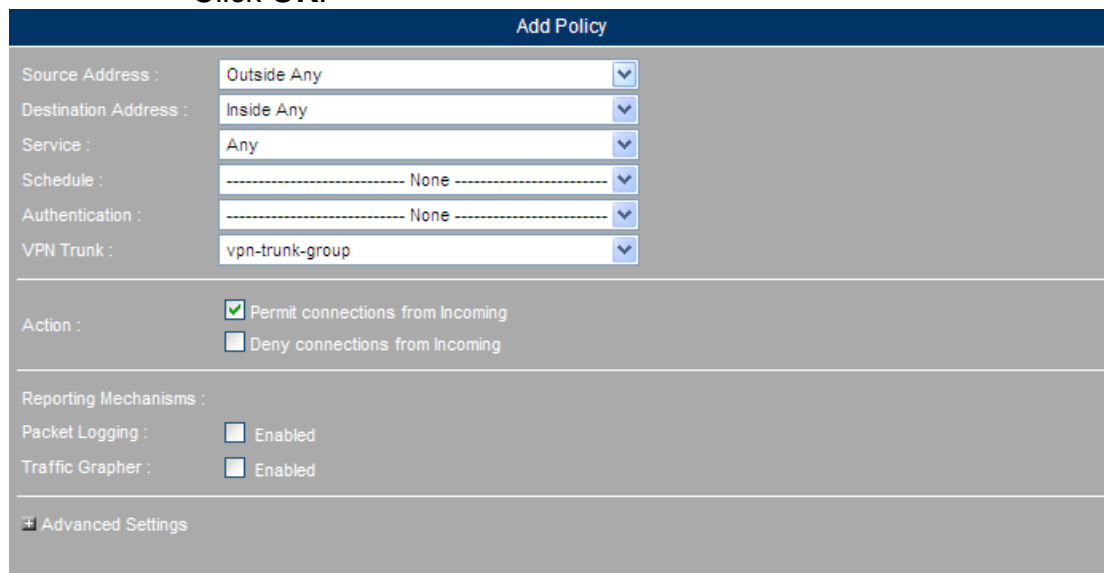
⏮ ⏪ ⏩ ⏭ / 1 Go ⏮ ⏪ ⏩ ⏭

New Entry

Policy Created

Step21. Go to **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.



Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

☐ Advanced Settings

Configuring an Incoming Policy with VPN Trunk

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

Total entries : 1

Policy Created

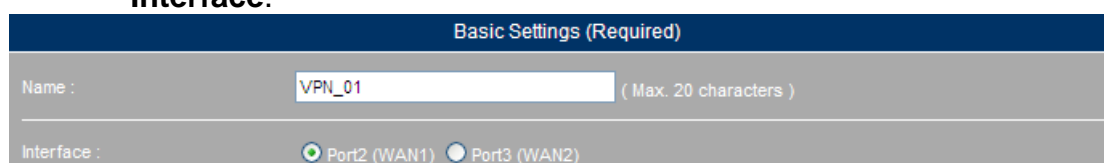
For B Company, set as shown below:

Step 1. Go to **Policy Object > VPN > IPSec Autokey** and then click the **New Entry** button.

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

The IPSec Autokey Page

Step 2. Type VPN_01 in the **Name** field and then select Port2(WAN1) for **Interface**.



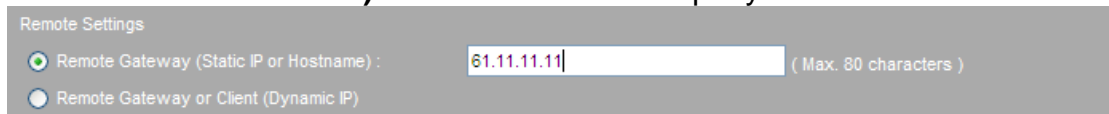
Basic Settings (Required)

Name : (Max. 20 characters)

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2)

Configuring the Name and the Interface

Step 3. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then enter A Company's IP.



Remote Settings

☒ Remote Gateway (Static IP or Hostname) : (Max. 80 characters)

☐ Remote Gateway or Client (Dynamic IP)

Configuring the Remote Settings

Step 4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.



Authentication Method :

Pre-Shared Key String : (Max. 62 characters)

Configuring the Authentication Method

Step 5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH for **Key Group**.



Encryption and Data Integrity Algorithms [Help](#)

ISAKMP Settings

Encryption Algorithm :

Authentication Algorithm :

Key Group :

Configuring the ISAKMP Algorithm

Step 6. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.



IPSec Settings

☒ Use both algorithms

Encryption Algorithm :

Authentication Algorithm :

☐ Use authentication algorithm only

Configuring the IPSec Algorithm

Step 7. Under the **Advanced Settings (optional)** section, select GROUP 1 for **PFS Key Group**, enter 3600 in the **ISAKMP SA Lifetime** field, enter 28800 in the **IPSec SA Lifetime** field and then select Main mode for **Mode**.



PFS Key Group :

ISAKMP SA Lifetime : seconds (1200 - 86400)

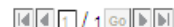
IPSec SA Lifetime : seconds (1200 - 86400)

IKE Negotiation : ☒ Main Mode ☐ Aggressive Mode

Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step 8. Setting completed.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_01	WAN1	61.11.11.11	3DES / MD5	—	Modify Remove



[New Entry](#)

IPSec Setting Completed

Step 9. Under **Policy Object > VPN > Trunk**, click the **New Entry** button and then set as shown below:

- Type the name in the **Name** field.
- **Local Settings**: Select LAN. **Local IP / Netmask**: Enter the subnet and the mask.
- Under the **Remote Settings** section, select **Remote IP / Netmask** and then enter the subnet and mask.
- Move VPN_01 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click **OK**.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

=====Available Tunnels=====

[Add >>](#)

[<< Remove](#)

=====Applied Tunnels=====

VPN_01


Keepalive IP Address :

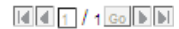
☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

[OK](#) [Cancel](#)

Configuring the Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.20.0 / 24	192.168.0.0 / 24	VPN_01	Modify Remove



[New Entry](#)

Setting Completed

Step 10. Go to **Policy Outgoing**, click the **New Entry** button and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.


Add Policy

Source Address :	Inside Any ▼
Destination Address :	Outside Any ▼
Service :	Any ▼
Schedule :	----- None ----- ▼
Authentication :	----- None ----- ▼
VPN Trunk :	ipsec-vpn-trunk ▼
Action : <input checked="" type="checkbox"/> Permit All <input type="checkbox"/> Deny All	
Reporting Mechanisms :	
Packet Logging :	<input type="checkbox"/> Enabled
Traffic Grapher :	<input type="checkbox"/> Enabled
Web Filter : ----- None ----- ▼	
Application Blocking : ----- None ----- ▼	
<input type="checkbox"/> Advanced Settings	

[OK](#) [Cancel](#)

Configuring an Outgoing Policy with VPN Trunk

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1 ▼

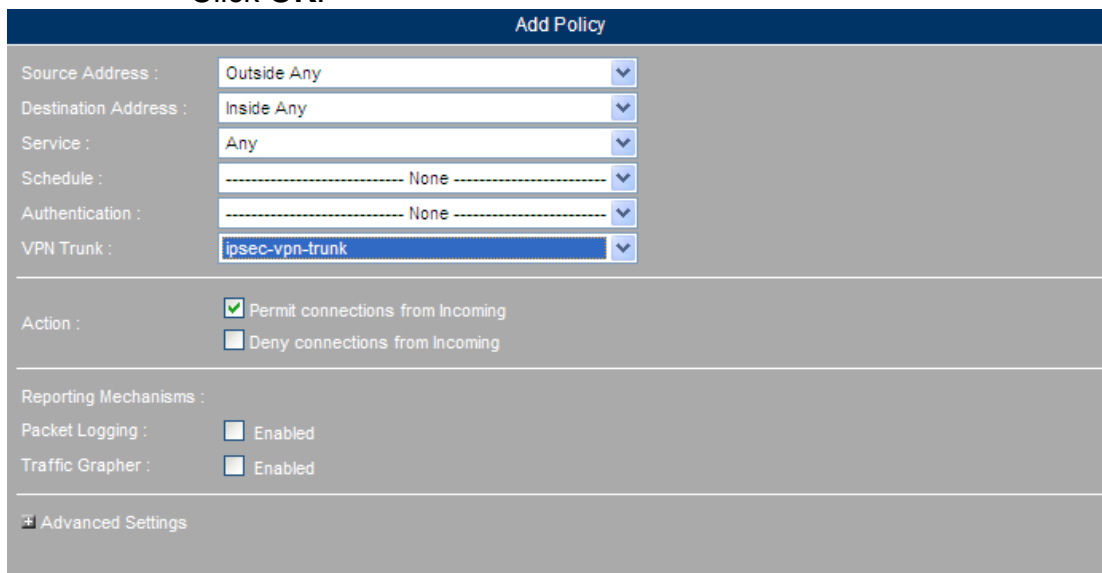


[New Entry](#)

A Policy with VPN Trunk Created

Step 11. Go to **Policy > Incoming**, click the **New Entry** button and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.



Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

☐ Advanced Settings

Configuring an Incoming Policy with VPN Trunk

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

A Policy with VPN Trunk Created

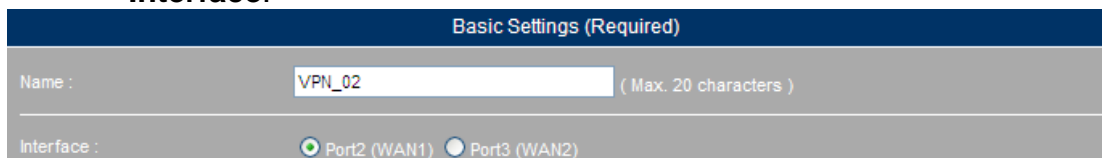
For C Company, set as shown below:

Step 1. Under **Policy Object > VPN > IPSec Autokey**, click the **New Entry** button and then set as shown below:

Status	Name	Interface	Gateway	Algorithm	Uptime	Configuration
No data found!						

The IPSec Autokey Page

Step 2. Enter the name in the **Name** field and then select Port2(WAN1) for **Interface**.



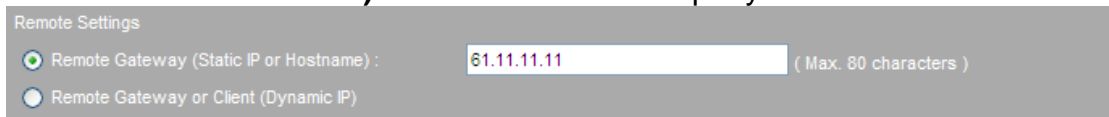
Basic Settings (Required)

Name : (Max. 20 characters)

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2)

Configuring the Name and the Interface

Step 3. Under the **Remote Settings** section, select **Remote Gateway (Static IP or Hostname)** and then enter A Company's IP in the field.



Configuring the Remote Settings

Step 4. Select Pre-Shared Key for **Authentication Method** and then enter the **Pre-Shared Key String**.



Configuring the Authentication Method

Step 5. Under the **ISAKMP Algorithm** section, select 3DES for **Encryption Algorithm**, select MD5 for **Authentication Algorithm** and then select DH for **Key Group**.



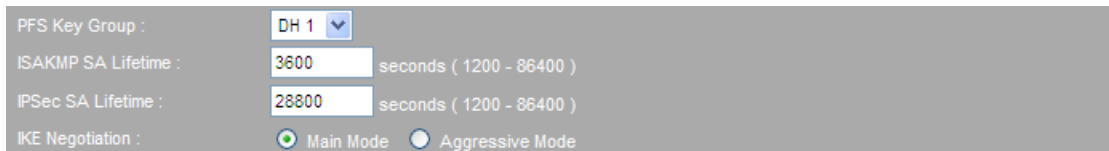
Configuring the ISAKMP Algorithm

Step 6. Under the **IPSec Algorithm** section, select **Use both algorithms**. Select 3DES for **Encryption Algorithm** and then select MD5 for **Authentication Algorithm**.




Configuring the IPSec Algorithm

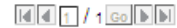
Step 7. Under the **Advanced Settings (optional)** section, select GROUP 1 from the **PFS Key Group** drop-down list. Enter 3600 in the **ISAKMP SA Lifetime** field and then enter 28800 in the **IPSec SA Lifetime** field.



Configuring the PFS Key Group, ISAKMP SA Lifetime, IPSec SA Lifetime and Mode

Step 8. Setting completed.

Status	Name ▲	Interface	Gateway	Algorithm	Uptime	Configuration
	VPN_02	WAN1	61.11.11.11	3DES / MD5	—	Modify Remove



[New Entry](#)

Setting Completed

Step 9. Go to **Policy Object > VPN > Trunk**, click the **New Entry** button and then set as shown below:

- Type the name in the **Name** field.
- **Local Settings** : Select LAN. Enter C Company's subnet / mask 192.168.30.3 / 255.255.255.0 in the field.
- Under the **Remote Settings** section, type A Company's subnet / mask 192.168.0.0 / 255.255.255.0 in the field.
- Move VPN_02 from the **Available Tunnels** column to the **Selected Tunnels** column.
- Tick **Enable NetBIOS Broadcast over VPN**.
- Click OK.

Add VPN Trunk

Name : (Max. 20 characters)

Local Settings :

Interface: ☒ LAN ☐ DMZ

Local IP Address / Netmask : /

Remote Settings:

☒ Remote IP Address / Netmask : /

☐ Remote Client

Tunnel Selection

-----Available Tunnels-----

-----Applied Tunnels-----

VPN_02

Add >>

<< Remove

Keepalive IP Address :


☒ Enable NetBIOS Broadcast over VPN

☐ Split task traffic across tunnels

OK

Cancel

Configuring the Trunk

Status	Name ▲	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.30.0 / 24	192.168.0.0 / 24	VPN_02	Modify Remove



[New Entry](#)

Setting Completed

Step 10. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.

Add Policy

Source Address :

Destination Address :

Service :

Schedule :

Authentication :

VPN Trunk :

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

Application Blocking :

Advanced Settings

[OK](#) [Cancel](#)

Configuring an Outgoing Policy

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1



[New Entry](#)

Policy Completed

Step 11. Go to **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the defined Trunk from the **VPN Trunk** drop-down list.
- Click **OK**.

Add Policy

Source Address : Outside Any ▼

Destination Address : Inside Any ▼

Service : Any ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : ipsec-vpn-trunk ▼

Action : ☒ Permit connections from Incoming
☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

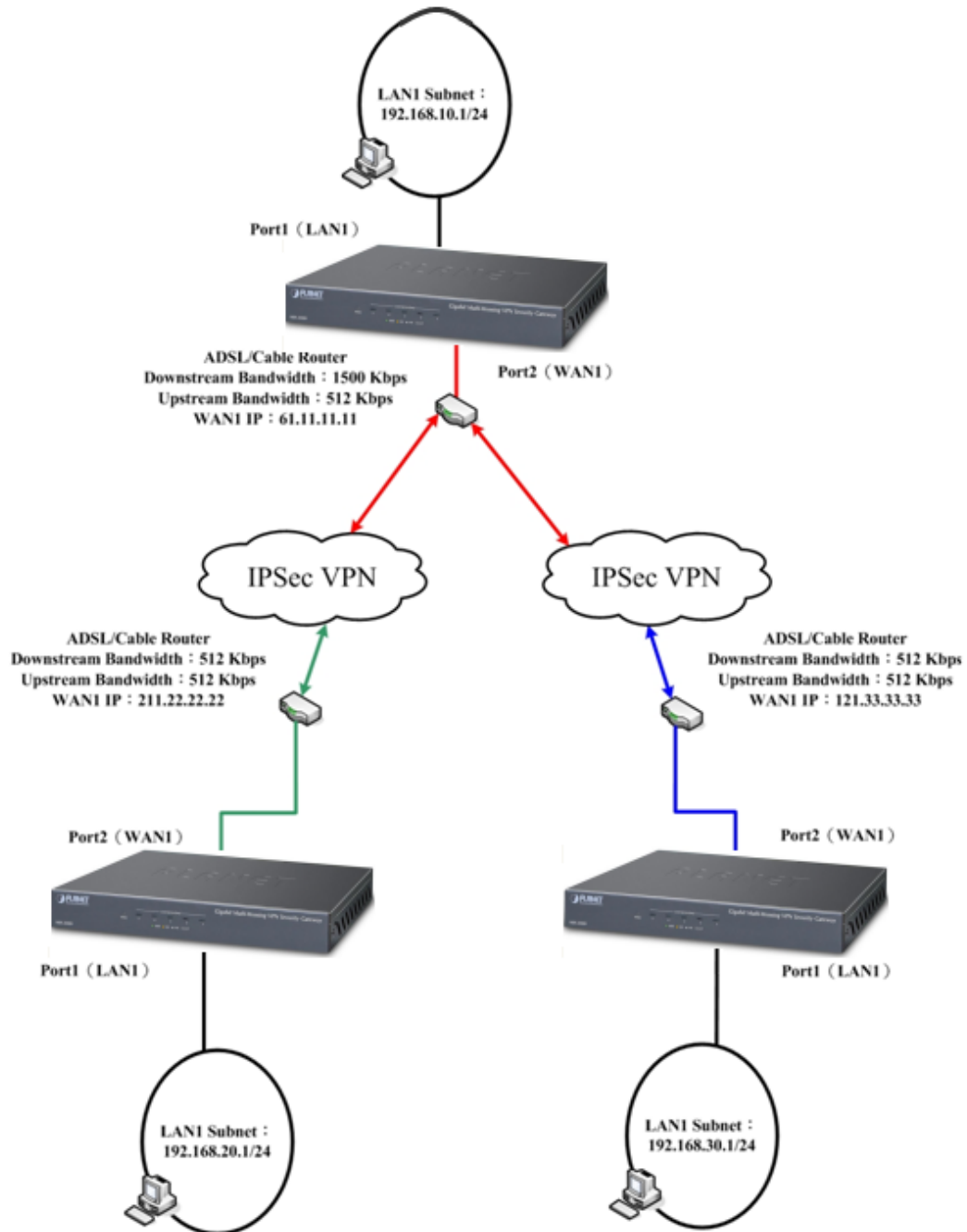
Advanced Settings

Configuring an Incoming Policy

Source	Destination	Service	Action	Options					Configuration			Priority
Outside Any	Inside Any	Any	VPN						Modify	Remove	Pause	1 ▼

Setting Completed

Step 12. Setting completed.



The Deployment of IPsec VPN

4.8.1.6 Using Two Units of MH-2300 to Load Balance Outbound PPTP VPN Traffic

Prerequisite Configuration (Note: The IP addresses are used as examples only)

[Company A]

Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Port 3 is defined as WAN 2 (61.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

[Company B]

Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x / 24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

Port 3 is defined as WAN 2 (211.33.33.33) and is connected to the Internet via the ADSL modem (ATUR).

Two PPTP VPN tunnels are established between Company A and B over their corresponding WAN 1 and WAN 2.

This example will be using two units of MH-2300 to establish VPN tunnels for private network access as follows:

For Company A, set as shown below:

Step 1. Go to **Policy Object > VPN > PPTP Server** and then set as shown below:

- Click the **Modify** button.
- Tick **Enable PPTP**.
- Tick **Encryption**.
- Tick **Allow Internet access via** and then select the port.
- **Auto-disconnect if idle for:** type 0.
- Enter the **Client IP – IP Range**.
- Click **OK**.

Modify PPTP Server

☒ Enable PPTP server

☒ Encryption

☒ Split Tunneling via

☐ Port1 (LAN1)

☒ Port2 (WAN1)

☒ Port3 (WAN2)

☒ Port4 (WAN3)

☐ Enable external RADIUS authentication

RADIUS Server IP or Hostname:

RADIUS Server Port:

RADIUS Server Shared Secret:

Auto-disconnect if idle for minute(s) (0 - 999999, 0: stays connected)

Echo Request Interval: second(s) (0 - 9, 0: disabled)

Timeout: second(s) (1 - 30)

Primary DNS Server:

Secondary DNS Server:


Primary WINS Server:

Secondary WINS Server:

Client IP Assignment

No.	Client IP / IP Range	Configuration
1	<input type="text" value="192.192.168.0"/> - <input type="text" value="255"/>	<input type="button" value="Next Row"/>

Enabling the PPTP Server



Note

1. The Internet access via PPTP VPN tunnel can be allowed or blocked when connecting to the MH-2300 from an external network.
2. **Auto-disconnect if idle for:** The PPTP VPN tunnels can be specified an idle timeout value (unit: minute) respectively to automatically disconnect.
3. To authenticate a PPTP VPN client using external RADIUS authentication (refer to Chapter 8 for related configuration), click **New Entry** to define RADIUS as the **Authentication Type** and add the client to the table under **Policy Object > VPN > PPTP Server**.

Step 2. Go to **Policy Object > VPN > PPTP Server** and then set as shown

276

below:

- Click **New Entry**.
- Select “Internal” for **Authentication Type**.
- Type “PPTP_01” in the **Username** field.
- Type “123456789” in the **Password** field.
- Select the radio box of “IP Range” under the **Client IP Assignment** section.
- Click **OK** to complete the settings.
- Click **New Entry** again.
- Select “Internal” for **Authentication Type**.
- Type in “PPTP_02” in the **Username** field.
- Type in “987654321” in the **Password** field.
- Select the radio box of “IP Range” under the **Client IP Assignment** section.
- Click **OK**.

Add PPTP Server

Authentication Type : Internal

Username : PPTP_01 (Max. 20 characters)

Password : (Max. 20 characters)

Client IP Assignment

☒ IP Range

☐ Static IP :

☐ Manual disconnection

OK
Cancel

Adding the First PPTP Server

PPTP Server (Disabled)
Modify

Status	Username	Client IP	Uptime	Configuration
	PPTP_01	0.0.0.0	---	Modify Remove

New Entry

The First PPTP Server Successfully Added

Add PPTP Server

Authentication Type : Internal

Username : PPTP_02 (Max. 20 characters)

Password : (Max. 20 characters)

Client IP Assignment

☒ IP Range

☐ Static IP :

☐ Manual disconnection



OK
Cancel

Adding the Second PPTP Server

PPTP Server (Disabled)

Modify

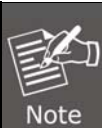
1 / 1 Go

Status	Username ▲	Client IP	Uptime	Configuration
	PPTP_01	0.0.0.0	---	<p>Modify Remove</p>
	PPTP_02	0.0.0.0	---	<p>Modify Remove</p>

1 / 1 Go

New Entry

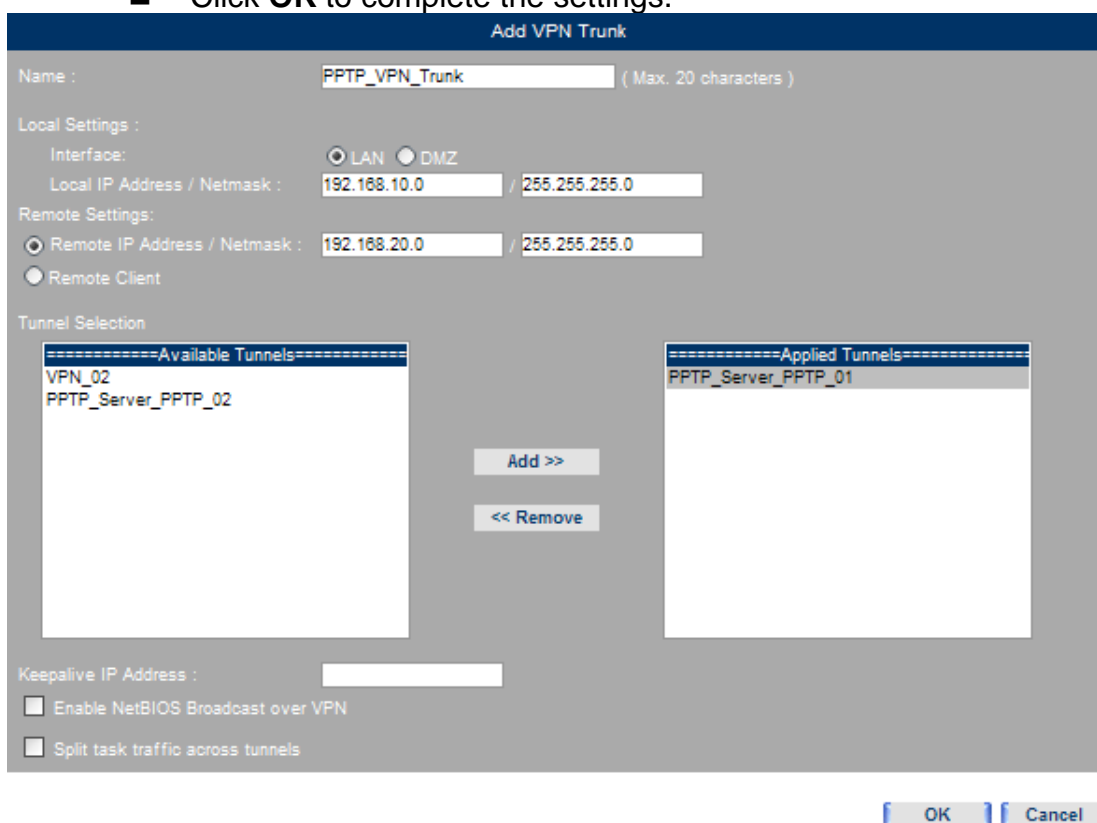
The Second PPTP Server Successfully Added



The PPTP server settings can be exported as a file for archiving and editing purpose, which can be used for restoring the list later on.

Step 3. Under **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:

- Specify a name for the VPN trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask of Company A.
- **Remote Settings :** Specify the subnet and netmask of Company B.
- Select “PPTP_Server_PPTP_01” from the **Available Tunnels** column on the left and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.



Adding a VPN Trunk

Status	Name	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	ipsec-vpn-trunk	192.168.30.0 / 24	192.168.0.0 / 24	VPN_02	Modify
	PPTP_VPN_Trunk	192.168.10.0 / 24	192.168.20.0 / 24	PPTP_Server_PPTP_01	Modify Remove

VPN Trunk Successfully Added



When specifying the **Remote IP Address / Netmask** for a PPTP VPN trunk, it merely takes a PPTP VPN tunnel to meet the requirement.

Step 4. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :	Inside Any
Destination Address :	Outside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	PPTP_VPN_Trunk

Action :
 ☒ Permit All
 ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled
 Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----
 Application Blocking : ----- None -----

☐ Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

/

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

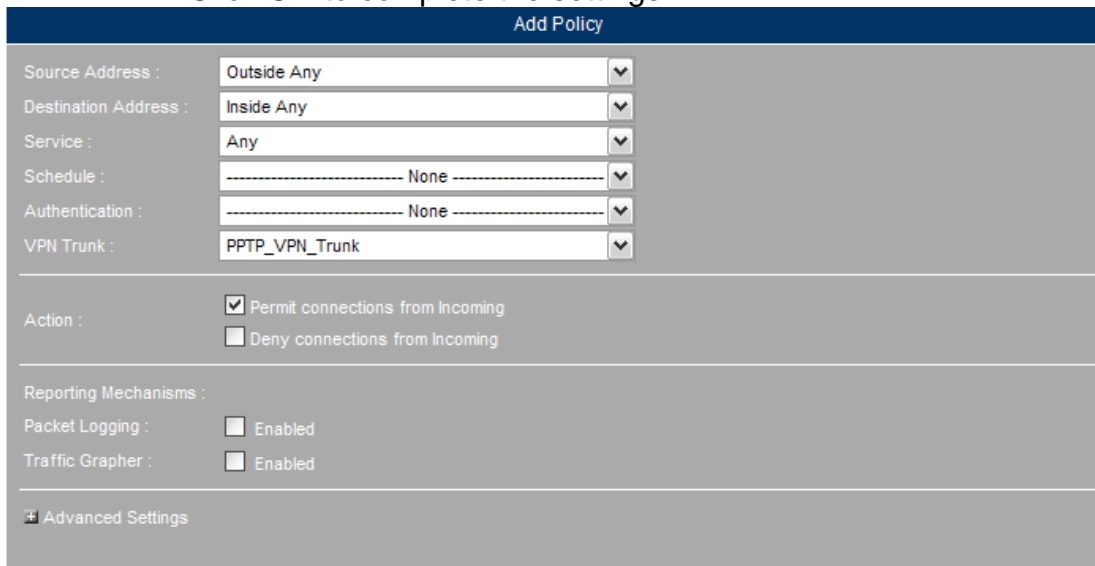
/

New Entry

Policy Successfully Created

Step 5. Go to **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.



OK Cancel

Creating a Policy to Apply the VPN Trunk Settings



Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		Modify Remove Pause	1

New Entry

Policy Successfully Created

For B Company, set as shown below:

Step 1. Go to **Policy Object > VPN > PPTP Client** and then set as shown below:

- Click **New Entry**.
- Type in "PPTP_01" in the **Username** field.
- Type in "123456789" in the **Password** field.
- Specify the WAN 1 gateway address of Company A in the **Server IP or Hostname** field.
- Tick the box of "Encryption".
- Select "Port2 (WAN1)" for **Interface**.
- Click **OK** to complete the settings.
- Click **New Entry** again.
- Type in "PPTP_02" in the **Username** field.
- Type in "987654321" in the **Password** field.
- Specify the WAN 2 gateway address of Company A in the **Server IP or Hostname** field.
- Tick the box of "Encryption".
- Select "Port3 (WAN2)" for **Interface**.

- Click **OK** to complete the settings.

Add PPTP Client

Username : (Max. 20 characters)

Password : (Max. 20 characters)

Server IP or Hostname : (Max. 80 characters) ☒ Encryption

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2) ☐ Port4 (WAN3)


☐ NAT with PPTP client [Help](#)

☐ Manual connection

[OK](#) [Cancel](#)

Adding the First PPTP Client

◀◀◀ 1 / 1 [Go] ▶▶▶

Status	Username ▲	Server IP or Hostname	Encryption	Uptime	Configuration
	PPTP_01	61.11.11.11	ON	---	Modify Remove

◀◀◀ 1 / 1 [Go] ▶▶▶

[New Entry](#)

First PPTP Client Successfully Added

Add PPTP Client

Username : (Max. 20 characters)

Password : (Max. 20 characters)

Server IP or Hostname : (Max. 80 characters) ☒ Encryption

Interface : ☐ Port2 (WAN1) ☒ Port3 (WAN2) ☐ Port4 (WAN3)



☐ NAT with PPTP client [Help](#)

☐ Manual connection

[OK](#) [Cancel](#)

Adding the Second PPTP Client

◀◀◀ 1 / 1 [Go] ▶▶▶

Status	Username ▲	Server IP or Hostname	Encryption	Uptime	Configuration
	PPTP_01	61.11.11.11	ON	---	Modify Remove
	PPTP_02	61.22.22.22	ON	---	Modify Remove

◀◀◀ 1 / 1 [Go] ▶▶▶

[New Entry](#)

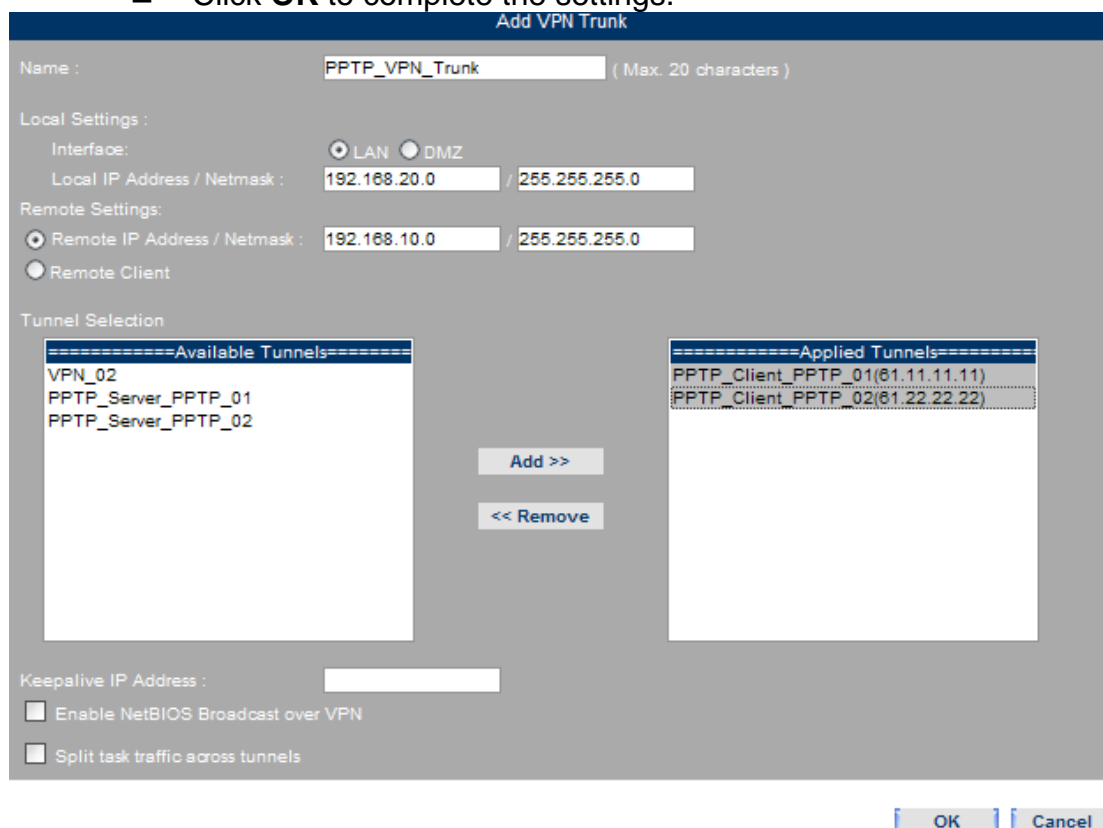
Second PPTP Client Successfully Added



The Internet access via PPTP VPN tunnel or the access to an IPSec VPN network requested by a PPTP VPN client needs to be achieved by ticking the box of "NAT with PPTP client".

Step 2. Under **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:


- Specify a name for the VPN trunk.
- **Local Settings:** Select “LAN” for **Interface** and specify the subnet and netmask for Company B.
- **Remote Settings :** Specify the subnet and netmask for Company A.
- Select “PPTP_Client_PPTP_01(61.11.11.11)” and “PPTP_Client_PPTP_02 (61.22.22.22)” from the **Available Tunnels** column on the left, and then click **Add**.
- Tick the box of “Enable NetBIOS Broadcast over VPN”.
- Click **OK** to complete the settings.



Adding a VPN Trunk

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		Modify Remove Pause	1

VPN Trunk Successfully Added



Note

When **Remote IP Address / Netmask** is used for **Remote Settings**, please refer to available number of WAN addresses to add the corresponding amount of PPTP VPN tunnels to the trunk setting.

Step 3. Go to **Policy > Outgoing** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :	Outside Any
Destination Address :	Inside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	PPTP_VPN_Trunk

Action :

☒ Permit connections from Incoming

☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

/ 1

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

/ 1

Policy Successfully Created

Step 4. Go to **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :	Outside Any
Destination Address :	Inside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	PPTP_VPN_Trunk

Action :

☒ Permit connections from Incoming

☐ Deny connections from Incoming

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

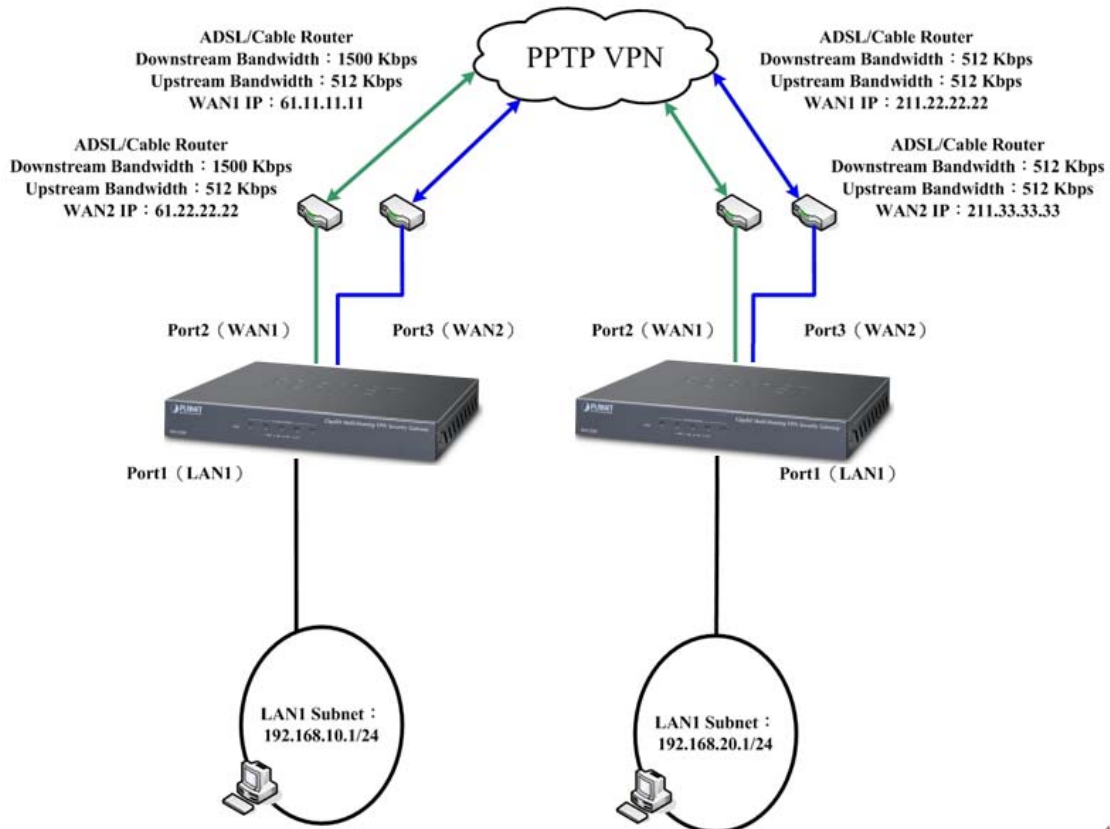
Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	Inside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

Policy Successfully Created

Step 5. PPTP VPN tunnels have been successfully established and load-balanced between the two sites.



The Deployment of a Load-balanced PPTP VPN Network between Two Units of MH-2300

4.8.1.7 Using Two Units of MH-2300 to Provide PPTP VPN Client with Internet Access via PPTP VPN Server

Prerequisite Configuration (Note: The IP addresses are used as examples only)

[Company A]

Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

[Company B]

Port 1 is defined as LAN 1 (192.168.20.1) and is connected to the LAN subnet 192.168.20.x / 24.

Port 2 is defined as WAN 1 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR).

This example will be using two units of MH-2300 to establish a VPN tunnel for providing the client-side users with Internet access as follows:

For Company A, set as shown below:

Step 1. Go to **Policy Object > VPN > PPTP Server** and then set as shown below:

- Click **Modify**.
- Tick the box of "Enable PPTP server".
- Tick the box of "Encryption".
- Tick the box of "Split Tunneling via" and then select the corresponding NIC port.
- Type in "0" in the **minute(s)** field to stay connected.
- Specify the **Client IP / IP Range** under the **Client IP Assignment** section.
- Click **OK** to complete the settings.

Modify PPTP Server

☒ Enable PPTP server
☒ Encryption
☒ Split Tunneling via

☐ Port1 (LAN1)
 ☒ Port2 (WAN1)
 ☐ Port3 (WAN2)
 ☐ Port4 (WAN3)

☐ Enable external RADIUS authentication
 RADIUS Server IP or Hostname:
 RADIUS Server Port:
 RADIUS Server Shared Secret:

Auto-disconnect if idle for: minute(s) (0 - 999999, 0: stays connected)
 Echo Request Interval: second(s) (0 - 9, 0: disabled)
 Timeout: second(s) (1 - 30)
 Primary DNS Server:
 Secondary DNS Server:
 Primary WINS Server:
 Secondary WINS Server:

Client IP Assignment

No.	Client IP / IP Range	Configuration
1	192.192.168.0 - 255	Next Row

Enabling the PPTP Server

Step 2. Go to **Policy Object > VPN > PPTP Server**, click **New Entry** and then set as shown below:

- Select “Internal” for **Authentication Type**.
- Type in “PPTP_Connection” in the **Username** field.
- Type in “123456789” in the **Password** field.
- Select the radio box of “IP Range” under the **Client IP Assignment** section.
- Click **OK** to complete the settings.

Add PPTP Server

Authentication Type : Internal

Username : PPTP_Connection (Max. 20 characters)

Password : (Max. 20 characters)

Client IP Assignment

☒ IP Range

☐ Static IP :

☐ Manual disconnection

OK
Cancel

Adding a PPTP Server

PPTP Server (Enabled)

Modify

1 / 1 Go

Status	Username ▲	Client IP	Uptime	Configuration	
	PPTP_Connection	0.0.0.0	---	Modify	Remove

1 / 1 Go

New Entry

PPTP Server Successfully Added

For Company B, set as shown below;

Step 1. Go to **Policy Object > VPN > PPTP Client**, click **New Entry** and then set as shown below:

- Type in "PPTP_Connection" in the **Username** field.
- Type in "123456789" in the **Password** field.
- Specify the WAN 1 gateway address of Company A in the **Server IP or Hostname** field.
- Tick the box of "Encryption".
- Select "Port2 (WAN1)" for **Interface**.
- Tick the box of "NAT with PPTP Client".
- Click **OK** to complete the settings.

Add PPTP Client

Username : (Max. 20 characters)

Password : (Max. 20 characters)

Server IP or Hostname : (Max. 80 characters) ☒ Encryption

Interface : ☒ Port2 (WAN1) ☐ Port3 (WAN2) ☐ Port4 (WAN3)

☒ NAT with PPTP client [Help](#)

☐ Manual connection


[OK](#) [Cancel](#)

Adding a PPTP Client

PPTP Server (Enabled)

[Modify](#)


1 / 1 [Go](#)

Status	Username ▲	Client IP	Uptime	Configuration
	PPTP_Connection	0.0.0.0	---	Modify Remove

1 / 1 [Go](#)

[New Entry](#)

PPTP Client Successfully Added



Note

The Internet access via PPTP VPN tunnel requested by a PPTP client needs to be achieved by ticking the box of "NAT with PPTP client"

Step 2. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:

- Specify a name for the VPN trunk.
- **Local Settings:** Select "LAN" for **Interface** and specify the subnet and netmask for Company B.
- **Remote Settings :** Specify the subnet and netmask for Company A.
- Select "PPTP_Client_PPTP_Connection(61.11.11.11)" from the **Available Tunnels** column on the left, and then click **Add**.
- Click **OK** to complete the settings.

Modify Trunk

Name : (Max. 20 characters)

Local Settings :
 Interface: ☒ LAN ☐ DMZ
 Local IP Address / Netmask : /

Remote Settings:
☒ Remote IP Address / Netmask : /
☐ Remote Client

Tunnel Selection

Available Tunnels

PPTP_Server_PPTP_Connection

Add >>

<< Remove

Applied Tunnels

PPTP_Client_PPTP_connection(61.11.11.11)


Keepalive IP Address :

☐ Enable NetBIOS Broadcast over VPN
☐ Split task traffic across tunnels

OK

Cancel

Adding a VPN Trunk

Status	Name	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	PPTP_VPN_Trunk	192.168.20.0 / 24	0.0.0.0 / 0	PPTP_Client_PPTP_conne...	<div style="background-color: #4CAF50; color: white; padding: 2px 5px;">Modify</div> <div style="background-color: #FF9800; color: white; padding: 2px 5px;">Remove</div>



New Entry

VPN Trunk Successfully Added

Step 3. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address :	Inside Any
Destination Address :	Outside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	PPTP_VPN_Trunk

Action : ☒ Permit All ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None -----

Application Blocking : ----- None -----

Advanced Settings

Creating a Policy to Apply the VPN Trunk Settings

1 / 1

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1

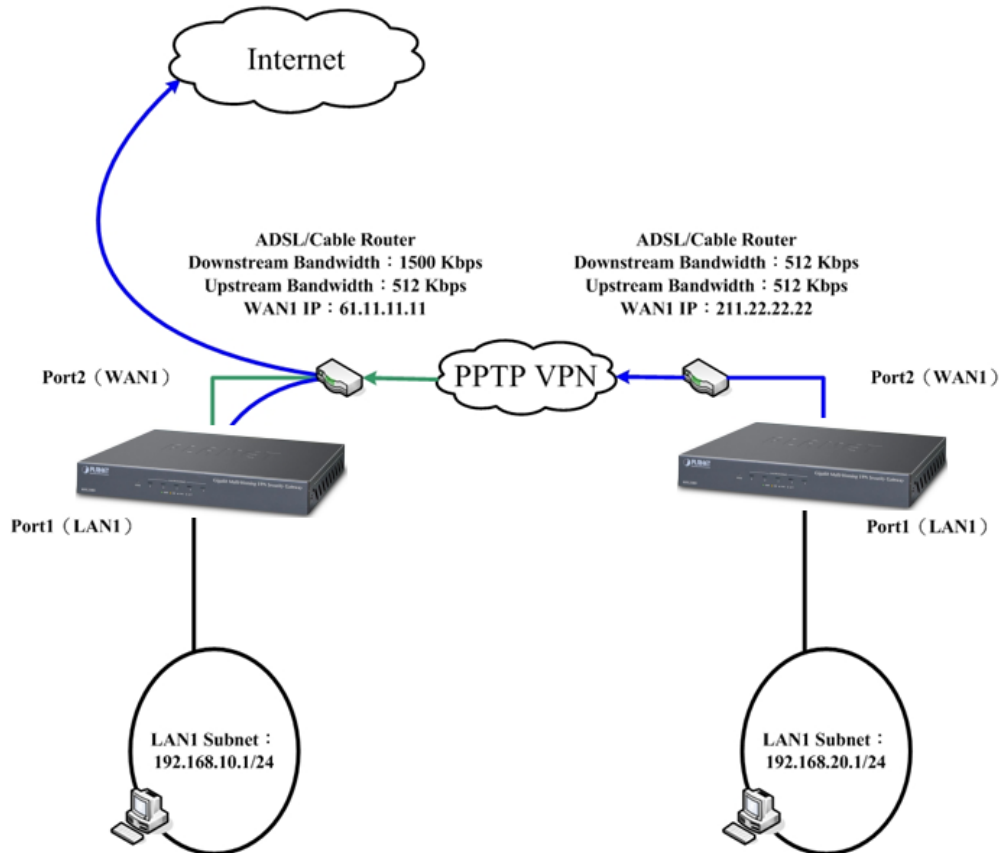
1 / 1

Policy Successfully Created

Note

This example merely requires the VPN trunk of Company B to be applied to an outgoing policy.

Step 4. PPTP VPN tunnel has been successfully established between the two sites, providing the client-side users with Internet access via the server-side MH-2300.



The Deployment of a PPTP VPN Network between Two Units of MH-2300 to Provide Client-side Users with Internet Access

4.8.1.8 Using a Unit of MH-2300 and a Windows 7 PC to Establish a PPTP VPN Tunnel

Prerequisite Configuration (Note: The IP addresses are used as examples only)

Company A is running a unit of MH-2300 with the following configuration:
Port 1 is defined as LAN 1 (192.168.10.1) and is connected to the LAN subnet 192.168.10.x / 24.

Port 2 is defined as WAN 1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR).

Company B is running a Windows 7 PC with an IP address of 211.22.22.22.

This example will be using a unit of MH-2300 and a Windows 7 PC to establish a VPN tunnel for private network access as follows.

For Company A, set as shown below:

Step 1. Go to **Policy Object > VPN > PPTP Server** and then set as shown below:

- Click **Modify**.
- Tick the box of "Enable PPTP server".
- Tick the box of "Encryption".
- Tick the box of "Split Tunneling via" and then select the corresponding NIC port.
- Type in "0" in the **minute(s)** field to stay connected.
- Specify the **Client IP / IP Range** under the **Client IP Assignment** section.
- Click **OK** to complete the settings.

Modify PPTP Server

☒ Enable PPTP server

☒ Encryption

☒ Split Tunneling via

☐ Port1 (LAN1)

☒ Port2 (WAN1)

☐ Port3 (WAN2)

☒ Port4 (WAN3)

☐ Enable external RADIUS authentication

RADIUS Server IP or Hostname:

RADIUS Server Port:

RADIUS Server Shared Secret:

Auto-disconnect if idle for minute(s) (0 - 999999, 0: stays connected)

Echo Request Interval: second(s) (0 - 9, 0: disabled)

Timeout: second(s) (1 - 30)

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Client IP Assignment

No.	Client IP / IP Range	Configuration
1	<input type="text" value="192.192.168.0"/> - <input type="text" value="255"/>	<input type="button" value="Next Row"/>

Enabling the PPTP Server



Note

1. The Internet access via PPTP VPN tunnel can be allowed or blocked when connecting to the MH-2300 from an external network.
2. The PPTP VPN tunnels can be specified an idle timeout value (unit: minute) respectively to automatically disconnect.
3. The access to an IPSec VPN network requested by a PPTP VPN client needs to be achieved by assigning a LAN 1 (192.168.10.x) address to the client-side user. In such a case, the PPTP VPN tunnel will be only accessible through the WAN address of IPSec VPN network.

Step 2. Under **Policy Object > VPN > PPTP Server**, click **New Entry** and then set as shown below:

- Select “Internal” for **Authentication Type**.
- Type in “PPTP_Connection” in the **Username** field.
- Type in “123456789” in the **Password** field.
- Select the radio box of “IP Range” under the **Client IP Assignment** section.
- Click **OK** to complete the settings.

Add PPTP Server

Authentication Type : Internal ▼

Username : PPTP_connection (Max. 20 characters)

Password : (Max. 20 characters)

Client IP Assignment

☒ IP Range

☐ Static IP :

☐ Manual disconnection

OK
Cancel

Adding a PPTP Server

Status	Username ▲	Client IP	Uptime	Configuration
	PPTP_connection	0.0.0.0	---	Modify Remove

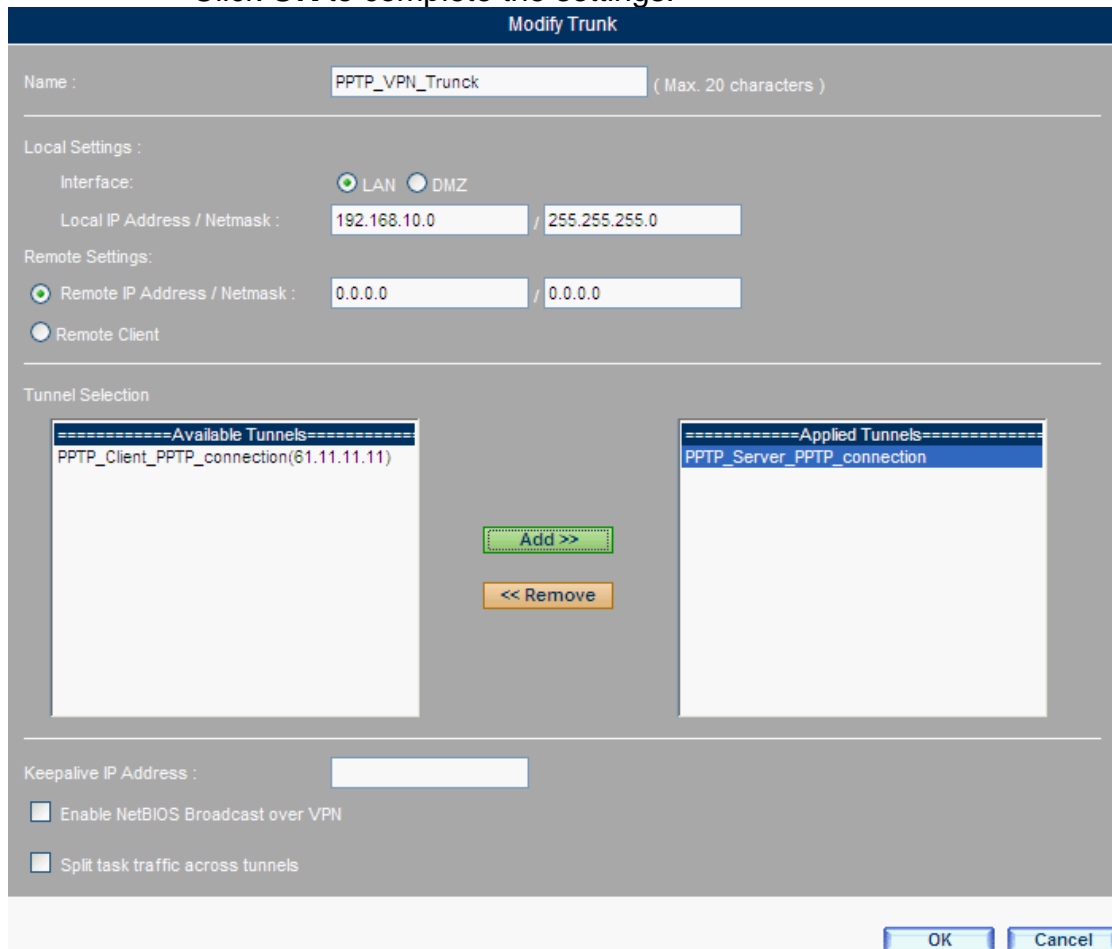


New Entry


PPTP Server Successfully Added

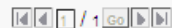
Step 3. Go to **Policy Object > VPN > Trunk**, click **New Entry** and then set as shown below:

- Specify a name for the VPN Trunk.
- **Local Settings:** Select "LAN" for **Interface** and specify the subnet and netmask for Company A.
- **Remote Settings :** Select **Remote Client**.
- Select "PPTP_Server_PPTP_Connection" from the **Available Tunnels** column on the left and then click **Add**.
- Tick the box of "Enable NetBIOS Broadcast over VPN".
- Click **OK** to complete the settings.



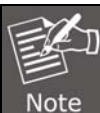
Creating a Trunk for the VPN Traffic

Status	Name	Local Subnet	Remote Subnet	Tunnel Selection	Configuration
	PPTP_VPN_Trunk	192.168.10.0 / 24	0.0.0.0 / 0	PPTP_Server_PPTP_conn...	Modify Remove



[New Entry](#)

Policy Successfully Created



The Local Settings from Step 3 must be specified with the LAN subnet of an IPsec VPN network if the access to it is requested by a PPTP VPN client.

Step 4. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.

Add Policy

Source Address : Inside Any ▼

Destination Address : Outside Any ▼

Service : Any ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : PPTP_VPN_Trunk ▼

Action :

☒ Permit All
 ☐ Deny All

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼

Application Blocking : ----- None ----- ▼

⚙️ Advanced Settings

OK
Cancel

Creating a Policy for Allowing Outgoing VPN Traffic

1 / 1

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	VPN		<div style="display: flex; justify-content: space-around; padding: 2px;"> Modify Remove Pause </div>	1 ▼

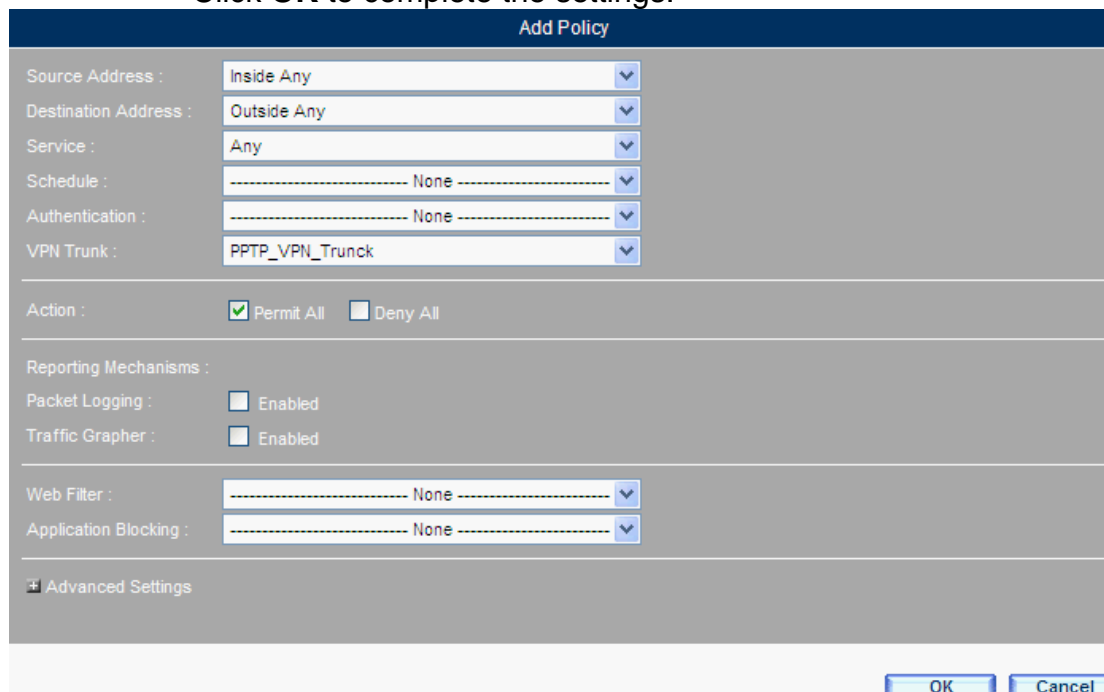
1 / 1

New Entry

Policy Successfully Created

Step 5. Under **Policy > Incoming**, click **New Entry** and then set as shown below:

- Select the VPN trunk for **VPN Trunk**.
- Click **OK** to complete the settings.



Creating a Policy for Allowing Incoming VPN Traffic

										1 / 1				
Source	Destination	Service	Action	Options						Configuration		Priority		
Inside Any	Outside Any	Any	VPN								Modify	Remove	Pause	1
										1 / 1				

New Entry

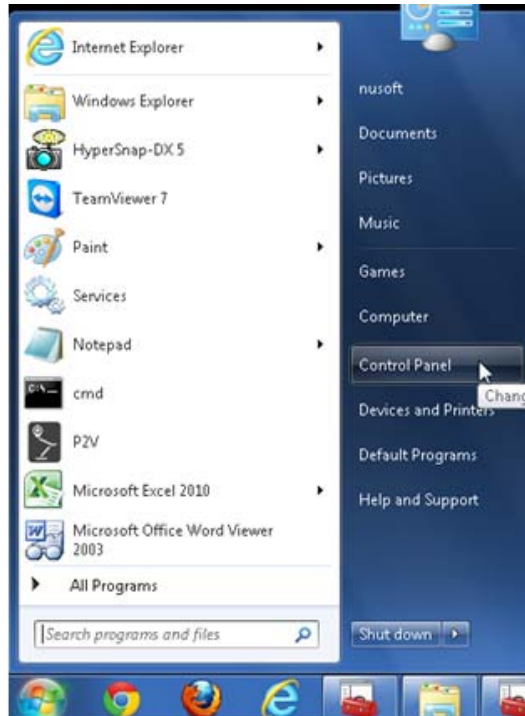
Policy Successfully Created

For B Company, set as shown below:

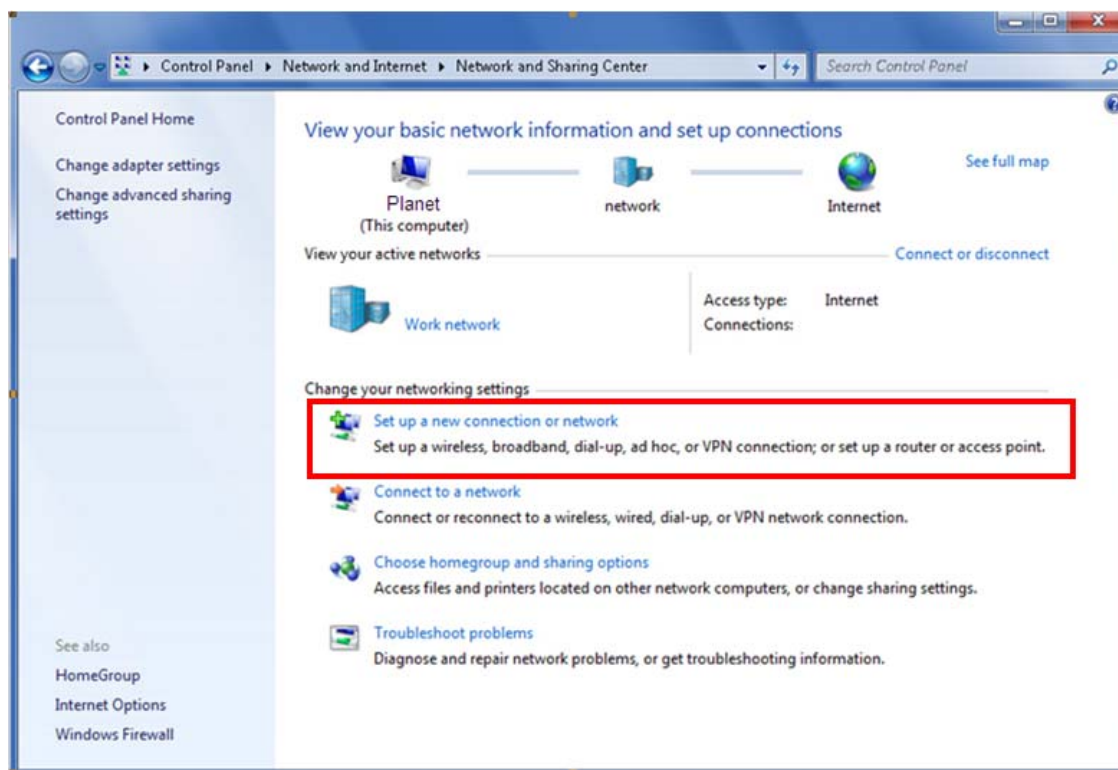
Step 1. Go to **Start > Control Panel > Network and Internet > Network and Sharing Center**, and then set as shown below:

- Select “Set up a new connection or network” under the **Change your networking settings** section.
- In the **Set Up a Connection or Network** dialog box:
 - ◆ Select “Connection to a workplace”.
 - ◆ Click **Next**.
- In the **Connect to a Workplace** dialog box:
 - ◆ Click **Use my Internet connection (VPN)**.
 - ◆ **Internet address:** Type in “61.11.11.11”.
 - ◆ **Destination name:** Specify a name.
 - ◆ Tick the box of “Don’t connect now, just set it up so I can connect later”.
 - ◆ Click **Next**.
 - ◆ Type in “PPTP_Connection” in the **User name** field.

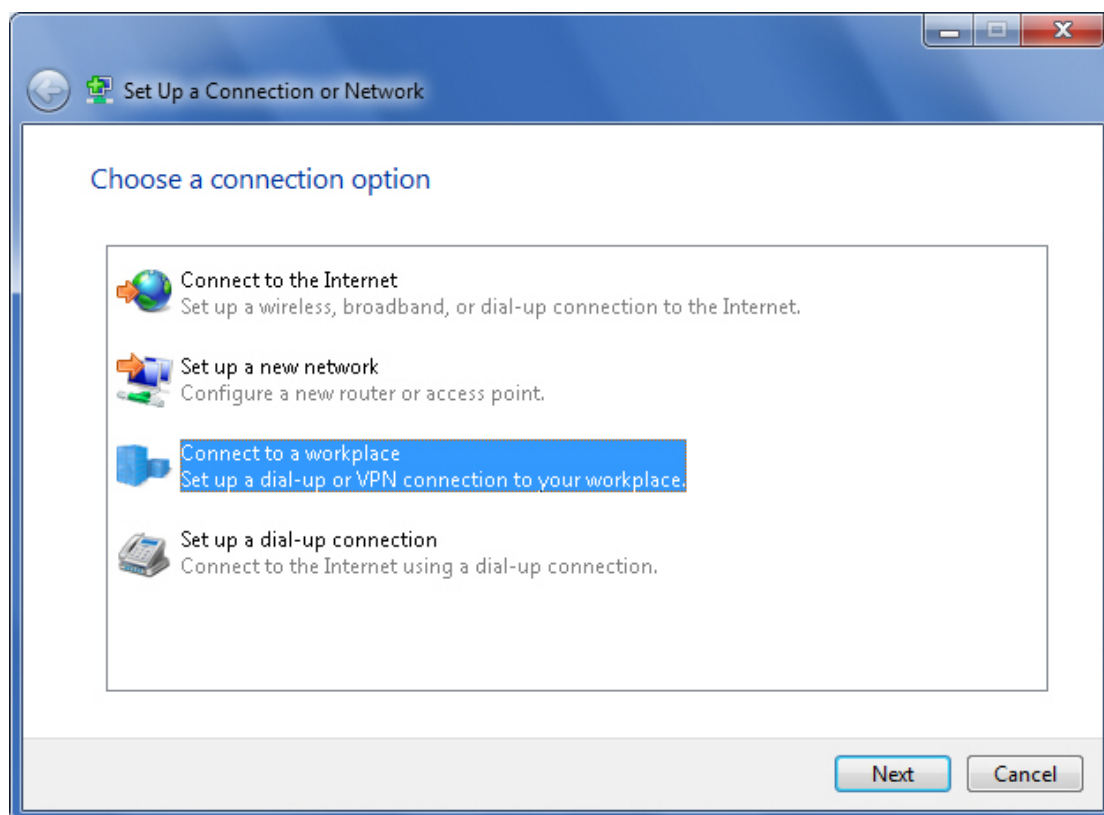
- ◆ Type in “123456789” in the **Password** field.
- ◆ Tick the box of “Remember this password”.
- ◆ Click **Create**.
- ◆ Click **Close**.
- Click **Change adapter settings** on the left panel:
- In the **Network Connections** window:
 - ◆ Right-click **VPN Connection** and select “Connect” from the shortcut menu.
 - ◆ In the **Connect VPN Connection** dialog box:
 - Click **Connect**.
 - ◆ The VPN Connection has been established successfully.



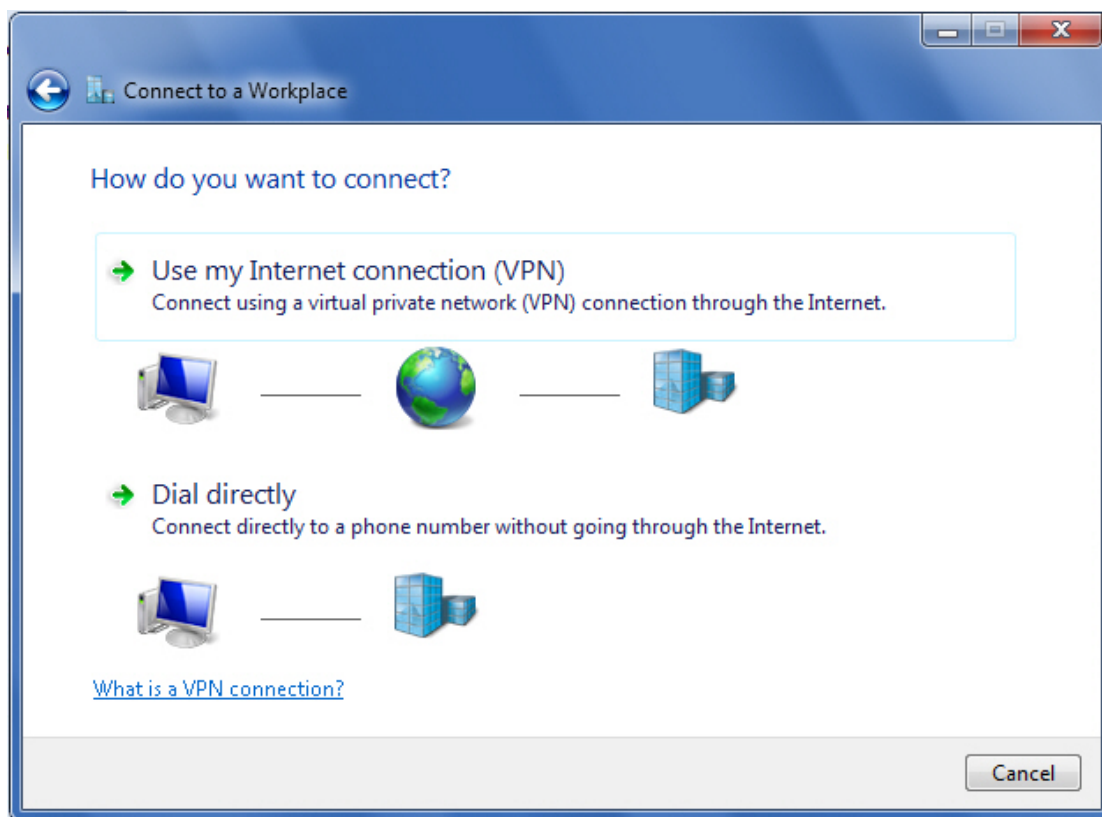
Selecting “Control Panel” on the Start Menu



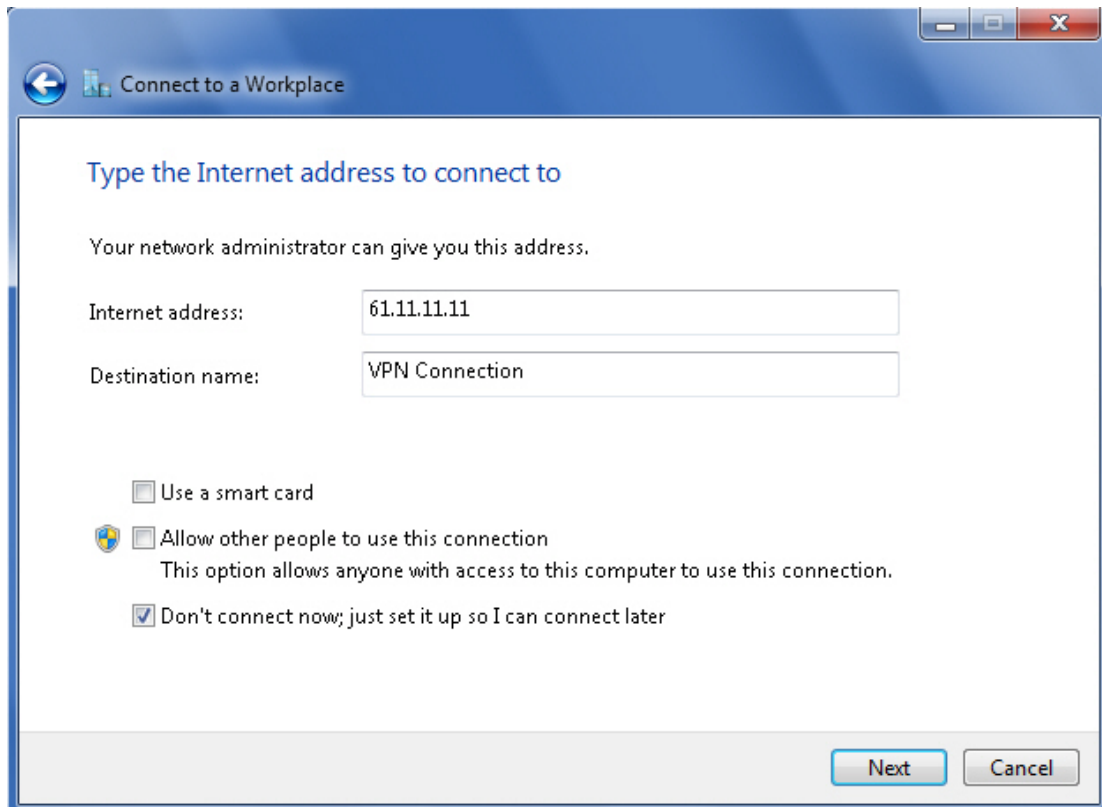
Selecting “Set up a new connection or network”



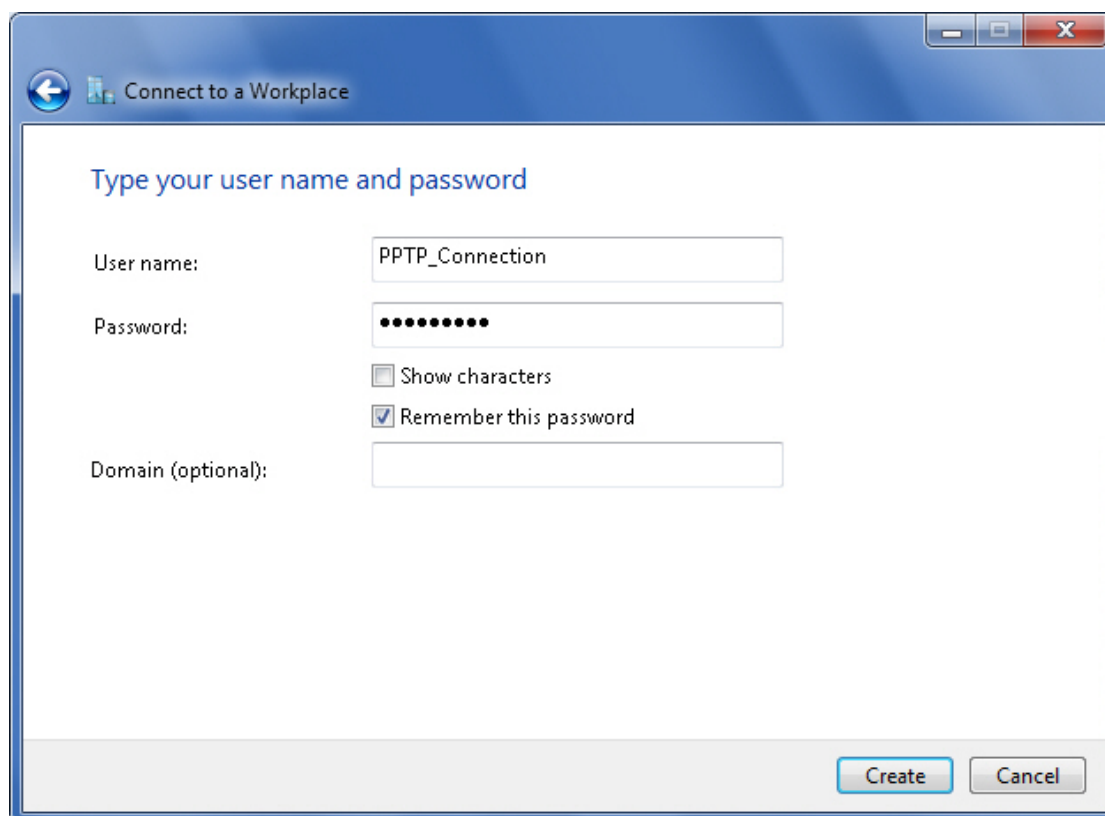
Selecting “Connect to a Workplace”



Choosing a Connection Method



Specifying an Internet Address to be Connected To



Connect to a Workplace

Type your user name and password

User name: PPTP_Connection

Password: ••••••••

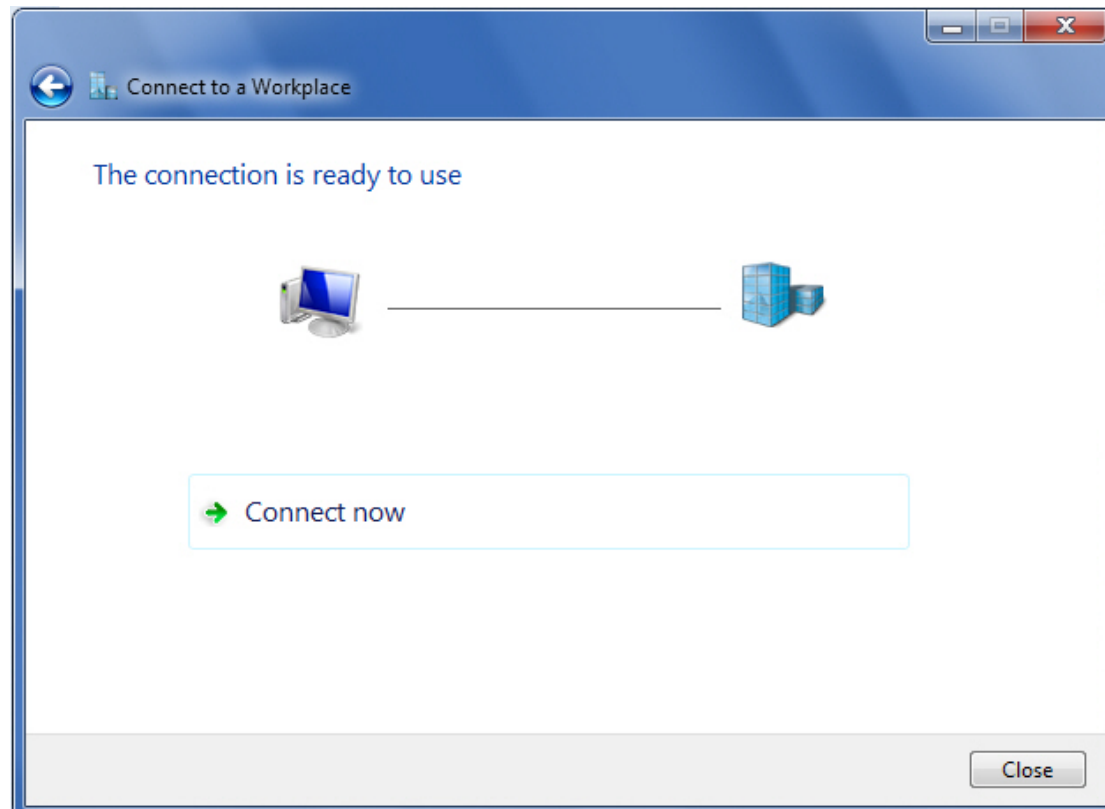
☐ Show characters

☒ Remember this password

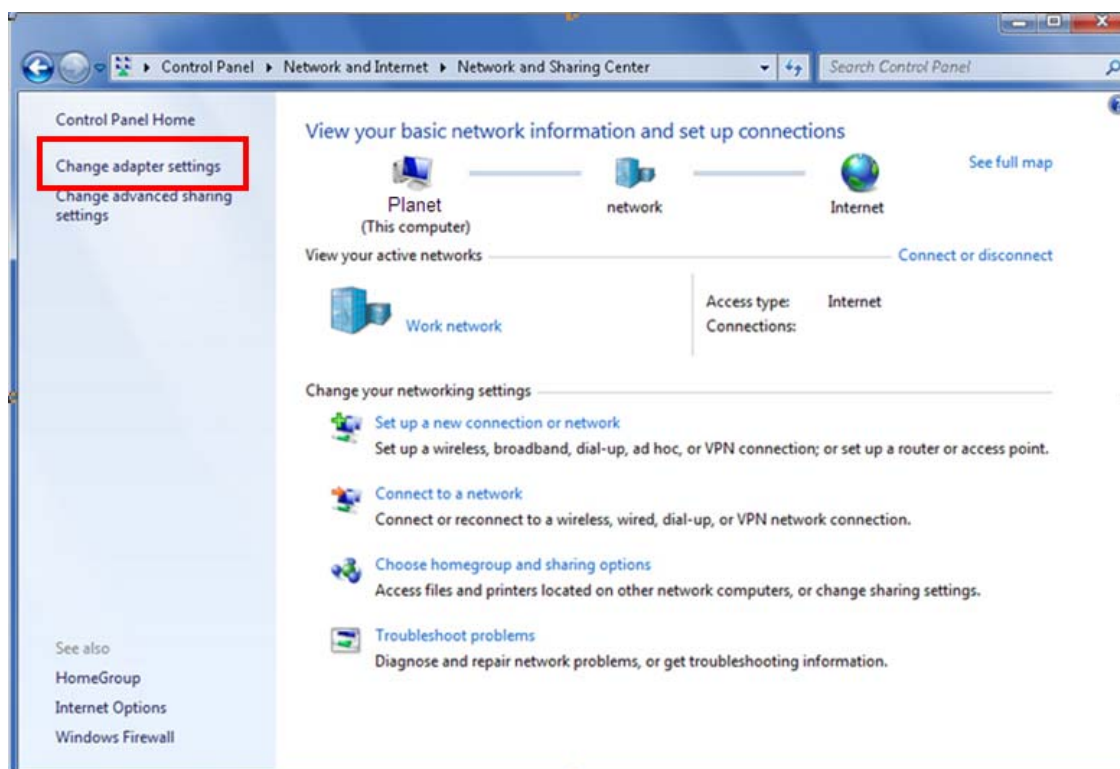
Domain (optional):

Create Cancel

Entering Your VPN Credentials in the Corresponding Fields



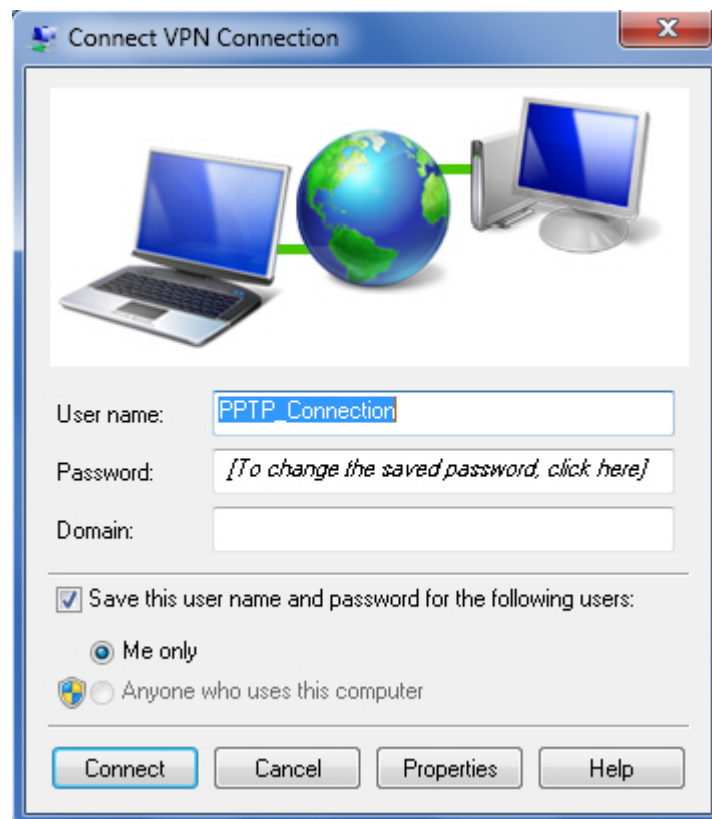
VPN Connectivity Configuration Successfully Completed



Selecting “Change Adapter Settings” on the Left Panel



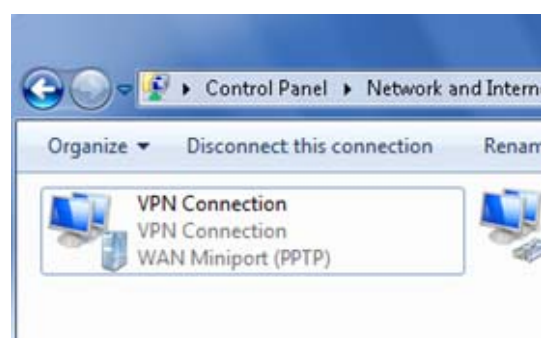
Right-clicking the VPN Connection Icon to Select “Connect” from the Shortcut Menu



Clicking “Connect” to Establish a VPN Connection

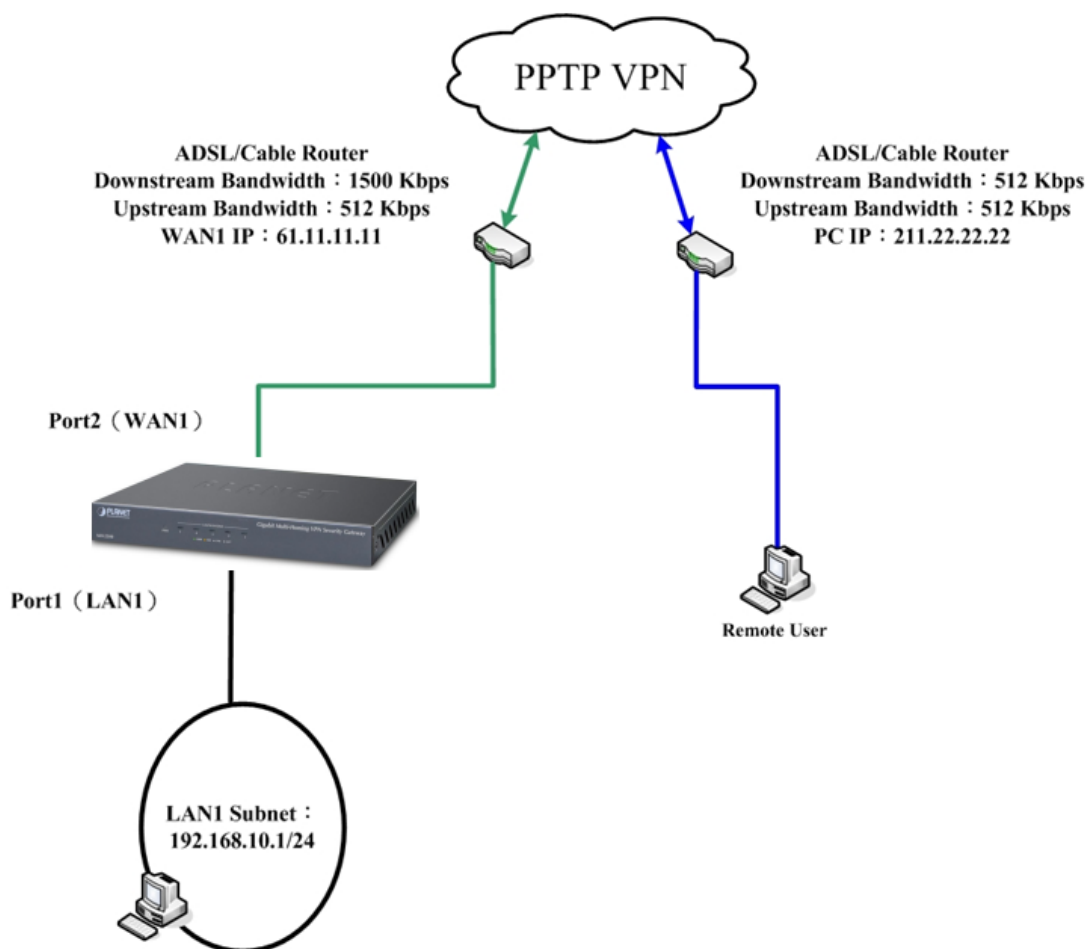


Verifying the VPN Credentials



VPN Connection Successfully Established

Step 2. PPTP VPN tunnel has been successfully established between the MH-2300 and the Windows 7 PC.



The Deployment of a PPTP VPN Network between MH-2300 and Windows7 PC

Chapter 5. Web Filter

5.1 Configuration

Websites, files, MIME types or scripting languages can be blocked to avoid cyberslacking or being affected by malicious codes (e.g., viruses) through the following means:

- **Whitelist** : Allows you to permit the access to a specific website using an exact URL address or a keyword along with a wildcard character “*”.
- **Blacklist** : Allows you to block the access to a specific website using an exact URL address or a keyword along with a wildcard character “*”.
- **File Extensions**: Allows you to block the HTTP or FTP file transfer based on their file extension.
- **MIME/Script**: Allows you to block the pop-up windows, ActiveX controls, Java applets and website cookies.
- **Group**: Allows you to group the filtering rules as per mentioned above to block the access to specific websites.

Terms in Settings

Alert Message Settings

- The users who attempt to access a blocked website will be presented with the customizable notification message.

Web Filter Log Settings

- The logs may be stored in the designated remote storage device.
 - ◆ Go to **Web Filter > Configuration > Settings** and then set as shown below:
 - Click **Enable message alerts for website blocking** and then enter the alert message to be displayed.
 - Click **OK**.

WCF Licensing Status

Status : Licensed

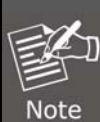
Expiration Date : 2011/1/31

Import a license key : **Alert Message Settings**☒ Enable message alerts for website blocking

Edit the alert message here :

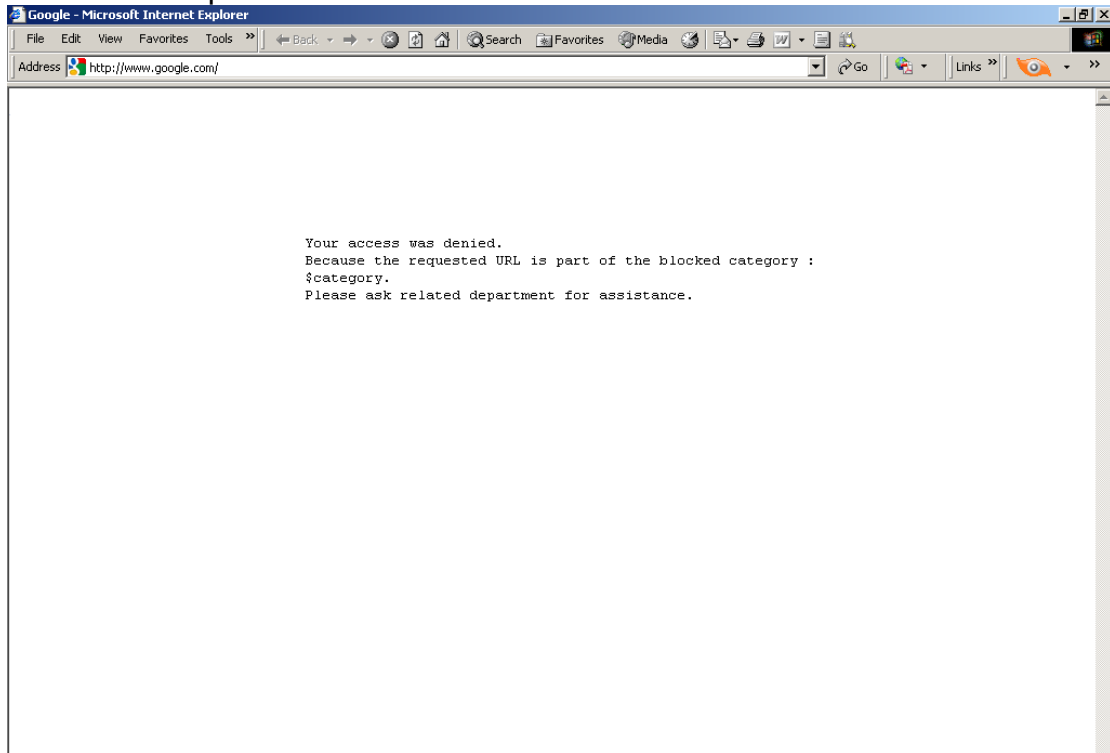
Your page request was denied because it is categorized as forbidden.
(Category: \$category) To gain access to it, please contact your network administrator.

- To inform users of the type of visited Web sites, you may insert the parameter ' \$category ' amongst the text in the message.

Web Filter Log SettingsStorage lifetime day(s) (1 - 99)☐ Enable Syslog**HTTP / FTP Virus Scanning**Max. File Scanning Size KB (10 - 5120)**The Web Filtering Settings**

Prior to enabling the syslog feature, please configure the **System Message Settings** under **System > Configuration > Settings**.

- ◆ Below is an alert message shown to an internal user who is in an attempt to visit a forbidden website.



The Denial Message for a Blacklisted Website

Terms in Whitelist

Name

- The name of a Whitelist rule.

URL

- Specifies a keyword or an exact URL address to permit the website access.
- To allow the access to all websites, type a wildcard "*" only.

Exclude File Extensions settings

- When ticked, files of specified extensions on the whitelisted website can be accessed.

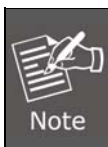
Terms in Blacklist

Name

- The name of a blacklist rule.

URL

- Specifies a keyword or an exact URL address to block the website access.
- To block the access to all websites, type a wildcard "*" only.



The filtering mechanisms are performed in the following order: Whitelist
Blacklist Group.

Terms in File Extensions

Name

- The name of a file extension rule.

Predefined File Extensions (Select All)

- Allows you to block the HTTP or FTP file transfer based on the selected predefined file extensions.

Custom File Extensions (Select All)

- Allows you to block the HTTP or FTP file transfer based on the selected custom file extensions.

All types of file extensions

- Allows you to block all HTTP or FTP file transfers.

Any file extensions used by downloaded manager software

- Allows you to block all file transfers processed through any downloaded manager.

Terms in MIME/Script

Name

- The name of an MIME/Script filtering rule.

Script

- Pop-up Window : Blocking pop-up windows.
- ActiveX Control : Disallowing the execution of ActiveX.
- Java Applet : Disallowing the execution of Java.
- Browser Cookie : Blocking website cookies.

MIME Type

- MIME (Multipurpose Internet Mail Extensions) is an Internet standard that extends the format of e-mail. It supports the binary contents and texts in character sets other than ASCII. In addition, it is also used for communication protocols such as HTTP.
- MIME is used to define the encoding method of an email message.
- "Content-Type" is used to the type of an email message using the header information, which can be categorized into two types:
 - ◆ Type:
 - ◆ Text: For filtering a text message that is composed of multiple charsets or formats.

- ◆ Multipart: For filtering a message that is composed of multiple subtypes.
- ◆ Application: For filtering any application or binary datagrams.
- ◆ Message: For constructing a MIME message.
- ◆ Image: For filtering any non-animated images.
- ◆ Audio: For filtering any audio packets.
- ◆ Video: For filtering any video packets.
- ◆ Subtype:
 - ◆ text/plain (for filtering a plain text document)
 - ◆ text/html (for filtering an HTML document)
 - ◆ application/xhtml+xml (for filtering an XHTML document)
 - ◆ image/gif (for filtering a GIF image)
 - ◆ image/jpeg (for filtering a JPEG image)
 - ◆ image/png (for filtering a PNG image)
 - video/mpeg (for filtering an MPEG video)
 - application/octet-stream (for filtering any octet datagrams)
 - application/pdf (for filtering a PDF document)
 - application/msword (for filtering an MS Word document)



Note

All the filtering rules, despite the type, are required to be applied to a group setting and then a policy.

5.1.1 Examples of Web Filter

5.1.1.1 Regulating the Website Access Through Whitelist and Blacklist Rule

Step 1. Go to **Web Filter > Configuration > Whitelist** and then set as shown below:

- Click **New Entry**.
- Specify a name in the **Name** field.
- In the **URL** field, type the keyword of the URL, such as “yahoo”.
- Click **OK**.
- Click **New Entry** again.
- Specify a name in the **Name** field.
- In the **URL** field, type the keyword of URL, such as “google”.
- Click **OK**.

Add Whitelist Entry

Name : (Max. 21 characters)

URL : (Max. 256 characters, ex. yahoo)

☐ Exclude File Extensions settings

OK

Cancel

Creating the First Whitelist Rule

Add Whitelist Entry

Name : (Max. 21 characters)

URL : (Max. 256 characters, ex. yahoo)

☐ Exclude File Extensions settings


Creating the Second Whitelist Rule

Export whitelist :

Import whitelist : (Max. file size: 1 MB)

Name ▲	URL ▲	File Access	Configuration
url_1	yah00	✗	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
url_2	google	✗	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Whitelist Rules Successfully Created



Whitelist rules can be exported as a file for storage, which can be used for restoring the list later on.

Step 2. Go to **Web Filter > Configuration > Blacklist** and then set as shown below:

- Specify a name in the **Name** field.
- In the **URL** field, enter *.
- Click **OK**.

Add Blacklist Entry

Name : (Max. 21 characters)

URL : (Max. 256 characters, ex. games)

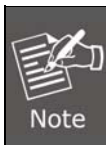
Creating a Blacklist Rule

Export blacklist :

Import blacklist : (Max. file size: 1 MB)

Name ▲	URL ▲	Configuration
url_3	*	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

Blacklist Rule Successfully Created



Blacklist rules can be exported as a file for storage, which can be used for restoring the list later on.

Step 3. Go to **Web Filter > Configuration > Group**, click **New Entry** and then set as shown below:

- Specify a name in the **Name** field.
- Move the Whitelist from the **Available Whitelists** column to the **Applied Whitelists** column.
- Move the Blacklist from the **Available Blacklists** column to the **Applied Blacklists** column.
- Click **OK**.

Add Group

Name : (Max. 21 characters)

Category :

Upload Blocking :

Download Blocking :

MIME / Script :

Whitelist

===== [Available Whitelists] =====

===== [Applied Whitelists] =====

url_1

url_2

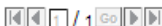
Blacklist

===== [Available Blacklists] =====

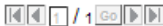
===== [Applied Blacklists] =====

url_3

Grouping Whitelist and Blacklist Rules



Group Name ▲	Group Items	Configuration
URL_Blocking_Group	Whitelist : url_1, url_2 Blacklist : url_3 Category : --- Upload Blocking : --- Download Blocking : --- MIME / Script : ---	<div>Modify Remove</div>



New Entry

The Group Setting for Web Filtering Rules

Step 4. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the defined group from the **Web Filter** drop-down list.
- Click **OK**.
- By applying this policy, only websites containing “yahoo” or “google” in the domain name will be permitted.

Add Policy

Source Address :	Inside Any
Destination Address :	Outside Any
Service :	Any
Schedule :	----- None -----
Authentication :	----- None -----
VPN Trunk :	----- None -----

☒ Permit All
 ☐ Deny All

Action :

Permit the selected:


☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (DMZ1)
 ☐ Permit Port 4 (WAN3)

Reporting Mechanisms :

Packet Logging : ☐ Enabled
 Traffic Grapher : ☐ Enabled

Web Filter : Web_Blocking_Group



Application Blocking : ----- None -----

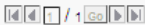
 Advanced Settings

OK

Cancel

Creating a Policy to Apply the Web Filtering Rules

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any			<div>Modify Remove Pause</div>	1 ▼



New Entry

Policy Successfully Created

5.1.1.2 Blocking the Website Access, HTTP / FTP File Transfers, and MIME / Script Types

Step 1. Go to **Web Filter > Configuration > File Extensions**, click **New Entry** and then set as shown below:

- Specify a name in the **Name** field.
- Select **All types of file extensions**.
- Click **OK**.

Add File Extension

Name : (Max. 20 characters)

☒ All types of file extensions
☐ Any file extensions used by download manager software

Forbidden File Extensions

Predefined File Extensions (☐ Select All)

<input type="checkbox"/> exe	<input type="checkbox"/> zip	<input type="checkbox"/> rar	<input type="checkbox"/> iso	<input type="checkbox"/> bin
<input type="checkbox"/> rpm	<input type="checkbox"/> doc	<input type="checkbox"/> xl.?	<input type="checkbox"/> ppt	<input type="checkbox"/> pdf
<input type="checkbox"/> tgz	<input type="checkbox"/> gz	<input type="checkbox"/> bat	<input type="checkbox"/> dll	<input type="checkbox"/> hta
<input type="checkbox"/> scr	<input type="checkbox"/> vb.?	<input type="checkbox"/> wps	<input type="checkbox"/> pif	<input type="checkbox"/> msi
<input type="checkbox"/> com	<input type="checkbox"/> reg	<input type="checkbox"/> mp3	<input type="checkbox"/> mp4	<input type="checkbox"/> mpeg
<input type="checkbox"/> mpg	<input type="checkbox"/> wma	<input type="checkbox"/> rmvb	<input type="checkbox"/> rm	<input type="checkbox"/> ram
<input type="checkbox"/> avi	<input type="checkbox"/> wmv	<input type="checkbox"/> 3gp	<input type="checkbox"/> mov	<input type="checkbox"/> asf
<input type="checkbox"/> amv				

Custom File Extensions

Creating a File Extension Rule

Available File Extensions :

<< < > >> / 1

Name ▲	File Extension	Configuration
WebCategory_Blocking	exe, zip, rar, iso, bin...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

<< < > >> / 1

The File Extension Rule for Blocking File Transfers

Note

- Under **Web Filter > Configuration > File Extensions**, file extensions can be added as shown in the following steps:
 - Click **Modify** next to **Available File Extensions** and then click **New Entry**.
 - Type the extension in the field.
 - Click **OK**.

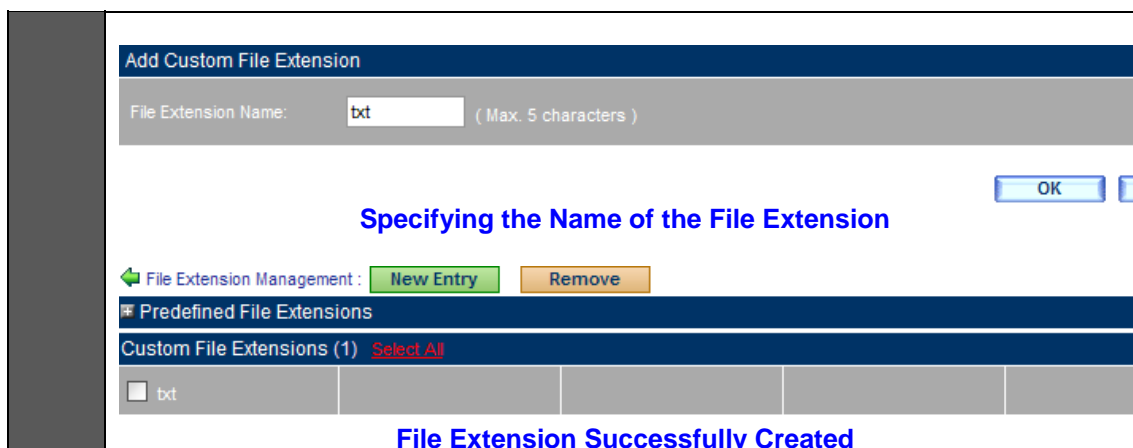
File Extension Management :

Predefined File Extensions

File Extension (0)

No data found!

Creating a File Extension



Add Custom File Extension

File Extension Name: (Max. 5 characters)

Specifying the Name of the File Extension

File Extension Management :

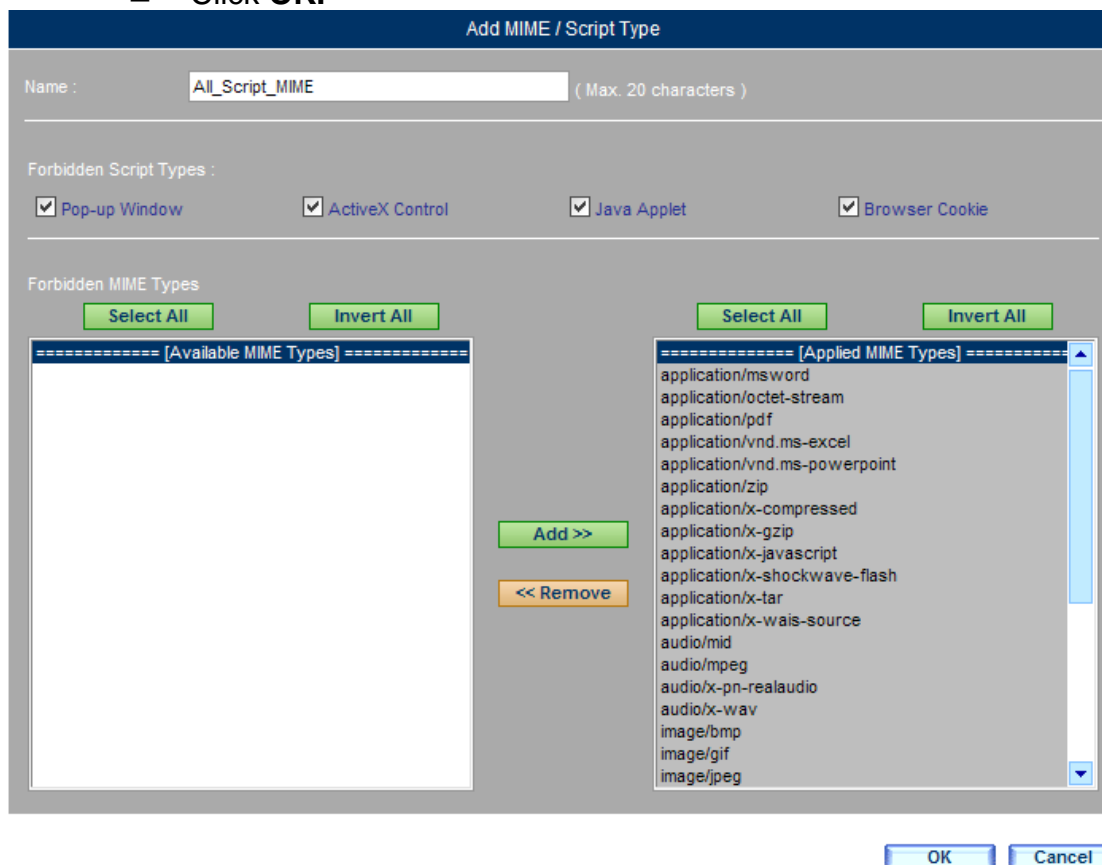
Predefined File Extensions

Custom File Extensions (1) [Select All](#)

<input type="checkbox"/> txt			
------------------------------	--	--	--

File Extension Successfully Created

- Step 2. Go to **Web Filter > Configuration > MIME/Script**, click **New Entry** and then set as shown below:
- Specify a name in the **Name** field.
 - Under the **Forbidden Script Types** section, tick **Pop-up Window**, **ActiveX Control**, **Java Applet** and **Browser Cookie**.
 - Move the MIME type from the **Available MIME Types** column to the **Applied MIME Types** column.
 - Click **OK**.



Add MIME / Script Type

Name : (Max. 20 characters)

Forbidden Script Types :

☒ Pop-up Window ☒ ActiveX Control ☒ Java Applet ☒ Browser Cookie

Forbidden MIME Types

===== [Available MIME Types] =====

===== [Applied MIME Types] =====

- application/msword
- application/octet-stream
- application/pdf
- application/vnd.ms-excel
- application/vnd.ms-powerpoint
- application/zip
- application/x-compressed
- application/x-gzip
- application/x-javascript
- application/x-shockwave-flash
- application/x-tar
- application/x-wais-source
- audio/mid
- audio/mpeg
- audio/x-pn-realaudio
- audio/x-wav
- image/bmp
- image/gif
- image/jpeg

Creating a MIME / Script Rule

Available MIME Types : [Modify](#) 1 / 1 [Go](#)


[Help](#)

Name	Forbidden Script Types	Forbidden MIME Types	Configuration
All_Script_MIME	Window Popup...	application/msword, application/octet-stream...	Modify Remove

1 / 1 [Go](#)

[New Entry](#)

The MIME / Script Rule for Blocking Scripting Languages


 Note

Under **Web Filter > Configuration > MIME/ Script**, MIME type can be added as in the following steps:

- Click **Modify** next to **Available MIME Types** and then click **Add**.
- Enter the **MIME Types** in the field.
- Click **OK**.

← MIME Types : [Add](#)

Predefined MIME Types

Forbidden MIME Types (0)

No data found!

Creating a MIME Type

Add MIME Type

Name: (Max. 30 characters, ex. test/test1)

[OK](#)

Specifying the Name of the MIME Type

← MIME Types : [Add](#) [Remove](#)

Predefined MIME Types

Custom MIME Types (1) [Select All](#)

<input type="checkbox"/> image/png		
------------------------------------	--	--

MIME Type Successfully Created

Step 3. Go to **Web Filter > Configuration > Group**, click **New Entry** and then set as shown below:

- Specify a name in the **Name** field.
- Select the defined rule from the **Upload Blocking** drop-down list and the **Download Blocking** drop-down list.
- Select the defined rule from the **MIME/Script** drop-down list.
- Click **OK**.

Modify Group

Name : (Max. 21 characters)

Upload Blocking :

Download Blocking :

MIME / Script :

Whitelist

===== [Available Whitelists] =====

===== [Applied Whitelists] =====

Blacklist

Select All **Invert All**

===== [Available Blacklists] =====

Select All **Invert All**

===== [Applied Blacklists] =====

Add >>

<< Remove

OK **Cancel**

Grouping the Filtering Rules

1 / 1 **Go**

Group Name ▲	Group Items	Configuration
Web_Blocking_Group	Whitelist : --- Blacklist : --- Upload Blocking : All_extend Download Blocking : All_extend MIME / Script : All_Script_MIME	<p>Modify Remove</p>

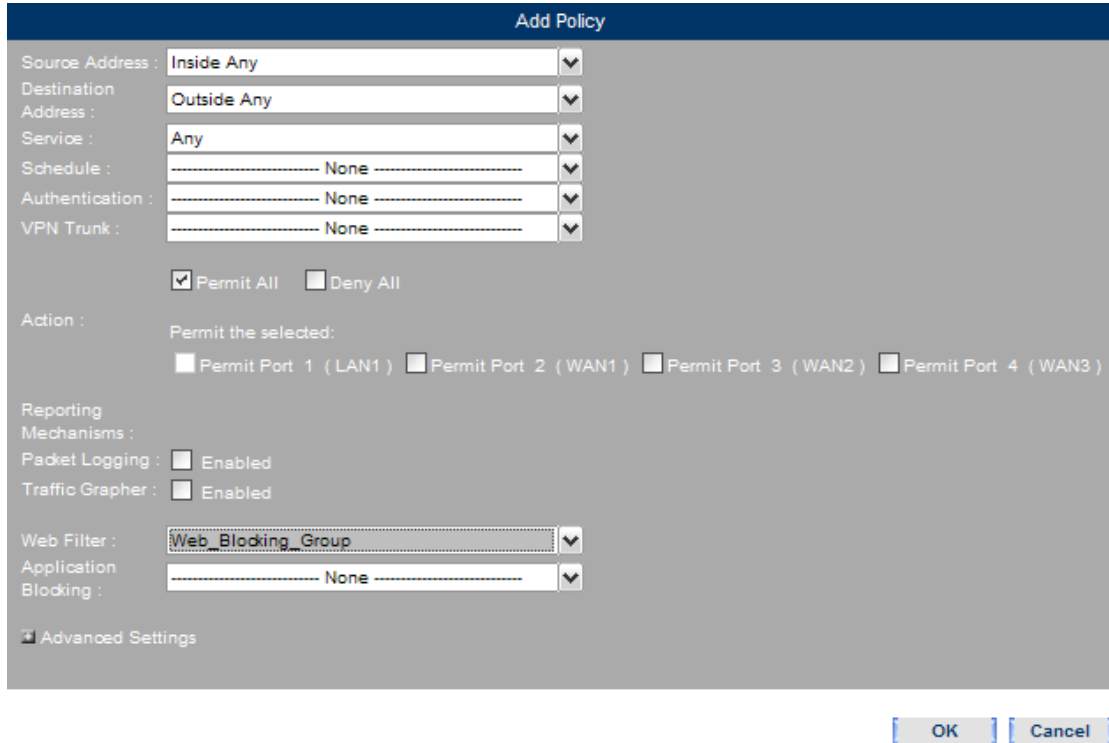
1 / 1 **Go**

New Entry

The Group Setting for Web Filtering Rules

Step 4. Go to **Policy > Outgoing**, click **New Entry** and then set as shown below:

- Select the defined group from the **Web Filter** drop-down list.
- Click **OK**.



Creating a Policy to Apply the Web Filtering Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✓	⊘	Modify Remove Pause	1

[New Entry](#)

Policy Successfully Created

5.2 Reports

Reports deliver you an insight into the website filtering operation with the detailed logs and statistics.

Terms in Settings


Periodic Report Scheduling Settings

- Generates and sends out a periodic report to the designated recipient(s) based on a schedule.
- Configures the maximum items per statistics chart.

Historical Report Scheduling Settings

- Generates the report of a specific date and instantly sends it to the designated recipient(s).

- ◆ Under **System > Configuration > Settings**, configure the **Email Notifications Settings**, and then refer to the following to adjust settings under **Web Filter > Reports > Settings**:
 - Under the **Periodic Report Scheduling Settings** section, tick **Enable the mailing of Periodic Report** and then select **Weekly report** and **Daily report**.
 - Click **OK**.
 - The recipient will receive the reports based upon the schedule.
 - Under the **Historical Report Scheduling Settings** section, specify the date to send the report.
 - Click **Send Report**.
 - The recipient will then receive the report(s).



Schedule for periodic report:

- Weekly report is produced at 00:00 hours on the first day of every week.
- Daily report is produced at 00:00 hours every day.

Periodic Report Scheduling Settings Help

☒ Enable the mailing of Periodic Report

☒ Weekly report ☒ Daily report

Max. Items per Statistics Chart: items (0: shows all available items)

Historical Report Scheduling Settings

☐ Weekly report ☐ Daily report

Report Frequency: (Please choose a frequency prior to the time selection.)


The Periodic Report Settings

@ inesc@planet.co... MH-2300(MH-2300) Daily Web Filter Report : (2014/12/16 ~ 2014/12/16) 2014/12/16 (Tue.) 上午 11:09

MH-2300(MH-2300) Daily Web Filter Report : (2014/12/16 ~ 2014/12/16)

inesc@planet.com.tw

Receiver: Ines / ENM Dept.

Attachment:  wf_daily_report.pdf (23 KB)

This report is generated by MH-2300.

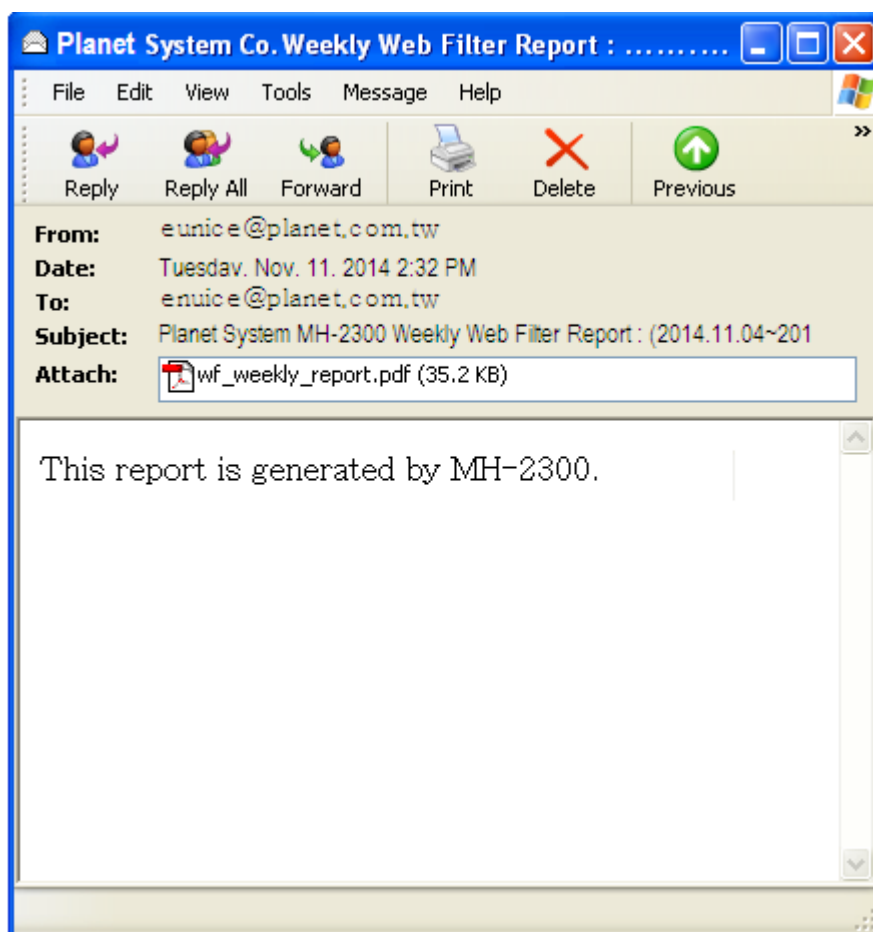
A Daily Report Sent through an Email Message

Historical Report Scheduling Settings

☒ Weekly report ☐ Daily report

Report Frequency: 2014/12/14 ~ 2014/12/20 

The History Report Settings



A Weekly History Report Sent through an Email Message

Planet System Co.					
Web Filter Weekly Report of : Website Category					
Website Category Top 20 Chart					
No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Whitelist	0	25952	25952	25952
2	Computers & Technology	0	24287	24287	24287
3	Unknown	0	23302	23302	23302
4	Search Engines & Portals	0	13328	13328	13328
5	General	0	8908	8908	8908
6	Information Security	0	8242	8242	8242
7	News	0	3990	3990	3990
8	Social Networking	0	3115	3115	3115
9	Advertisements & Pop-Ups	0	2689	2689	2689
10	Personal Sites	0	2676	2676	2676
11	Education	0	2323	2323	2323
12	Forums & Newsgroups	0	2211	2211	2211
13	Business	0	1513	1513	1513
14	Shopping	0	1479	1479	1479
15	Government	0	1142	1142	1142
16	Arts	0	963	963	963
17	Job Search	0	867	867	867
18	Transportation	0	747	747	747
19	Instant Messaging	0	734	734	734
20	Chat	0	734	734	734

The First Page of History Report

Terms in Logs

Search

- Category: Available searching criteria are time, source IP address, website, category and action.
- Upload: Available searching criteria are time, source IP address, website, filename, filtering rule and action.
- Download: Available searching criteria are time, source IP address, website, filename, filtering rule and action.
- MIME/Script: Available searching criteria are time, source IP address, website, filtering rule and action.
- ◆ Go to **Web Filter > Reports > Logs**, click the **Search** icon to start a search:
 - Enable the searching duration and specify a period of time to search within.
 - Select "All" for **Category**.
 - Select "All" for **Status**.
 - Click **Search**.
 - Click **Download** to store the result.

Search Web Filtering Logs

☒ Start a search from: 2010 / 12 / 24 00 : 00
 To : 2010 / 12 / 24 16 : 03
 Source IP : (ex. 192.168.1.10)
 Website Address : (Max. 256 characters)
 Category : All
 Action : All

Search

Results

2010-12-24(44 Records)

Download

Help

1 / 3 Go

Time	Source IP	Website Address	Category	Action
16:02:45	TEST-PC	download754.avast.com	Information Security	✓
16:02:11	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:02:09	TEST-PC	download754.avast.com	Information Security	✓
16:01:36	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:01:33	TEST-PC	download754.avast.com	Information Security	✓
16:01:33	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:01:00	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:00:57	TEST-PC	download754.avast.com	Information Security	✓
16:00:57	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:00:22	TEST-PC	rad.msn.com	Search Engines & Portals	✓
16:00:22	TEST-PC	download754.avast.com	Information Security	✓
16:00:20	TEST-PC	rad.msn.com	Search Engines & Portals	✓
15:59:46	TEST-PC	rad.msn.com	Search Engines & Portals	✓
15:59:46	TEST-PC	download923.avast.com	Information Security	✓
15:59:42	TEST-PC	rad.msn.com	Search Engines & Portals	✓
15:59:10	TEST-PC	download923.avast.com	Information Security	✓
15:59:08	TEST-PC	rad.msn.com	Search Engines & Portals	✓
15:59:06	TEST-PC	rad.msn.com	Search Engines & Portals	✓
15:58:34	TEST-PC	download923.avast.com	Information Security	✓
15:58:30	TEST-PC	rad.msn.com	Search Engines & Portals	✓

1 / 3 Go

Searching for the Specific Logs



Note

1. Under **Web Filter > Reports > Logs**, the **Category** reports can be sorted by the time, source IP, website address, category or action.
2. Under **Web Filter > Reports > Logs**, the **Downloaded and Uploaded** reports can be sorted by the time, source IP, website address, filename, filtering rule or action.
3. Under **Web Filter > Reports > Logs**, the **MIME/Script** reports can be sorted by the time, source IP, website address, filtering rule or action.

5.2.1 Statistics

Step 1. Under **Web Filter > Reports > Statistics**, bar charts shows the report of URL blocking.

- Click **Day** for daily statistical report.

- Click **Week** for weekly statistical report.
- Click **Month** for monthly statistical report.
- Click **Year** for yearly statistical report.

Year Month Week Day Date: 2010-12-24 Chart: Website Category

Website Category Top Chart

No.	Website Category	Blocked	Allowed	Total	Access Indicator
1	Information Security	0	40	40	40
2	Unknown	0	17	17	17
3	Search Engines & Portals	0	16	16	16
4	General	0	1	1	1
5	Computers & Technology	0	1	1	1
6	Web-based Email	0	1	1	1

Duration: 2010/12/24 00:00 ~ 2010/12/24 16:21 Total: 76 Average: 4.47 URLs/Hour

Website Address Top Chart

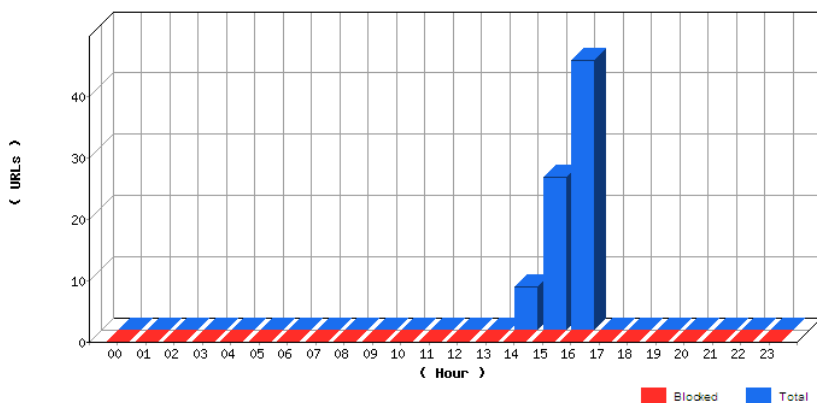
No.	Website Address	Blocked	Allowed	Total	Access Indicator
1	rad.msn.com	0	15	15	15
2	1002.avast.com	0	6	6	6
3	download789.avast.com	0	5	5	5
4	download754.avast.com	0	5	5	5
5	download682.avast.com	0	5	5	5
6	download728.avast.com	0	5	5	5
7	download923.avast.com	0	5	5	5
8	download516.avast.com	0	5	5	5
9	download667.avast.com	0	5	5	5
10	www.msfnets.com	0	2	2	2
11	tw.news.yahoo.com	0	2	2	2
12	lyimg.com	0	2	2	2
13	tools.google.com	0	1	1	1
14	sup.live.com	0	1	1	1
15	byfiles.storage.msn.com	0	1	1	1
16	207.46.125.52	0	1	1	1
17	207.46.124.166	0	1	1	1
18	www.google.com.tw	0	1	1	1
19	tw.yahoo.com	0	1	1	1
20	login.live.com	0	1	1	1

Duration: 2010/12/24 00:00 ~ 2010/12/24 16:21 Total: 76 Average: 4.47 URLs/Hour

NetBIOS Name / IP Address Top Chart

No.	NetBIOS Name / IP Address	Blocked	Allowed	Total	Access Indicator
1	TEST-PC	0	69	69	69
2	ENMLAB-PC	0	7	7	7

Duration: 2010/12/24 00:00 ~ 2010/12/24 16:21 Total: 76 Average: 4.47 URLs/Hour



5.2.2 Logs

Step 1. Under **Web Filter > Reports > Logs**, there it shows the URL blocking logs.

Browse logs by: Category 2010-12-24(84 Records) Help 1 / 5 Go

Time	Source IP	Website Address	Category	Action
16:25:41	TEST-PC	download651.avast.com	Information Security	✓
16:25:05	TEST-PC	download651.avast.com	Information Security	✓
16:24:29	TEST-PC	download651.avast.com	Information Security	✓
16:23:51	TEST-PC	download807.avast.com	Information Security	✓
16:23:15	TEST-PC	download807.avast.com	Information Security	✓
16:22:40	TEST-PC	download807.avast.com	Information Security	✓
16:22:04	TEST-PC	download807.avast.com	Information Security	✓
16:21:28	TEST-PC	download807.avast.com	Information Security	✓
16:20:50	TEST-PC	download789.avast.com	Information Security	✓
16:20:14	TEST-PC	download789.avast.com	Information Security	✓
16:19:38	TEST-PC	download789.avast.com	Information Security	✓
16:19:02	TEST-PC	download789.avast.com	Information Security	✓
16:18:27	TEST-PC	download789.avast.com	Information Security	✓
16:17:57	TEST-PC	tools.google.com	Unknown	✓
16:17:49	TEST-PC	download667.avast.com	Information Security	✓
16:17:13	TEST-PC	download667.avast.com	Information Security	✓
16:16:37	TEST-PC	download667.avast.com	Information Security	✓
16:16:01	TEST-PC	download667.avast.com	Information Security	✓
16:15:25	TEST-PC	download667.avast.com	Information Security	✓
16:14:47	TEST-PC	ll002.avast.com	Information Security	✓

1 / 5 Go Clear

The Web Filtering Logs

Chapter 6. Policy

6.1 Policy

MH-2300 inspects each packet passing through the device to see if it meets the criteria of any policy. Every packet is processed according to the designated policy; consequently any packets that do not meet the criteria will not be permitted to pass.

The items of a policy include Source Address, Destination Address, Service, Schedule, Authentication, VPN Trunk, Action, Packet Log, Traffic Grapher, Web Filter, Application Blocking, QoS, Max. Bandwidth per Source IP, P2P Bandwidth Limits, Max. Concurrent Sessions per IP, Max. Concurrent Sessions, Traffic Quota per Session, Quota per Source IP, Traffic Quota per Day, IP Redirection, etc. The IT administrator could determine the outgoing and incoming service or application of which data packets should be blocked or processed by configuring these items.

The IT administrator can customize the policy based on the source address, source port, destination address and destination port of a packet. According to the attribute of a packet, the policy setting is categorized into:

- **Outgoing:** Applied to the traffic that are from the LAN and heading to the WAN.
- **Incoming:** Applied to the traffic that are from the WAN and heading to the LAN (e.g., originated from a mapped IP or virtual server).
- **WAN to DMZ:** Applied to the traffic that are from the WAN and heading to the DMZ (e.g., originated from a mapped IP or virtual server).
- **LAN to DMZ :** Applied to the traffic that are from the LAN and heading to the DMZ.
- **DMZ to WAN :** Applied to the traffic that are from the DMZ and heading to the WAN.
- **DMZ to LAN :** Applied to the traffic that are from the DMZ and heading to the LAN.
- **LAN to LAN :** Applied to the traffic that are from the LAN and heading to the LAN.
- **DMZ to DMZ:** Applied to the traffic that are from the DMZ and heading to the DMZ.



1. MH-2300 packets are only processed when the criteria of a network policy are met. Consequently, connections between any two networks require a policy to be established.
2. VPN connections established by MH-23001000 can be aggregated into a trunk as well as applied to a network policy so as to manage the access privileges.

Terms in Policy

Source Address & Destination Address









- Source address and Destination address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.
- For a quick modification of **address**, **Mapped IPs**, **Port Mapping** and **Port-Mapping Group** settings, click the IP address in the **Source** or **Destination** column.

Service


- The service to be regulated. Available options are the system default services and the customized services.
- To modify the service settings, click the service in the **Service** column.

Options


- It shows the function that has been activated. When a function is activated, the symbol corresponding to it will appear (see the table below).

Symbol	Meaning	Description
	Schedule	The policy is applied as scheduled. scheduled.
	Authentication	Authentication is applied to the policy.
	Packet Logging	Packet logging is activated by the policy.
	Traffic Grapher	Traffic grapher is activated by the policy.
	Web Filter	Web filtering is activated by the policy.
	Application	Application blocking is activated by the policy.
	QoS	QoS is activated by the policy.
	IP Redirection	The source address in the packets processed by the policy will carry a translated IP or their original IP based on the selected option: Automatic, Routing or NAT.

Schedule

- The time at which a policy executes.
- To modify the schedule settings, click the schedule icon  in the **Options** column.

Authentication







- This requires users to be authenticated to create a connection.
- To modify the schedule settings, click the schedule icon  in the **Options** column.

VPN Trunk



- This is where you apply the policy to regulate the session packets of IPSec or PPTP VPN.

Action


- It determines over which WAN interfaces/ packets are permitted to pass through (see the table below).

Symbol	Meaning	Description
	Allowed to pass through all WAN interfaces	Packets that meet the criteria of the policy are allowed to pass through the WAN interfaces..
	Allowed to pass through WAN 1 interface	Packets that meet the criteria of the policy are allowed to pass through WAN 1. interface.
	Allowed to pass through WAN 2	Packets that meet the criteria of the policy are allowed to pass through WAN 2. .
	Allowed to pass over VPN Trunk	Only VPN packets that meet the criteria of the policy are allowed.
	Access denied	Packets that meet the criteria of the policy will be denied.
	Paused	The policy is currently suspended.


Packet Logging

- Records the packet transmissions managed by the policy, such as Protocol, Port, Source IP, Destination IP, etc. To see the logs, click the Packet Logging icon .
- To view a packet log, click the packet logging icon  in the **Options** column.


Traffic Grapher

- When enabled, there will be a chart drawn from the statistics of traffic flow.
- To view a traffic graph, click the traffic grapher icon  in the **Options** column.


Web Filter

- Restricts the use of HTTP or FTP protocol.
- To modify the web filter settings, click the icon  in the **Options** column.

Application Blocking


- Blocks the use of instant messaging, peer-to-peer sharing, video / audio streaming, Web-based email messaging, online gaming, VPN tunneling, remote controlling and other applications.
- To modify the application blocking settings, click the icon  in the **Options** column.

QoS

- The guaranteed and maximum bandwidth settings. (Note: The bandwidth is allocated to users that meet the criteria of the policy.)
- To modify the QoS settings, click the icon  in the **Options** column.

Max. Bandwidth per Source IP

- Limits the bandwidth of each IP address respectively.

 Note	<ol style="list-style-type: none"> 1. When the total sum of Max. Bandwidth per Source IP has reached the maximum bandwidth of QoS, there will be no spare bandwidth available for new sessions. 2. The Max. Bandwidth per Source IP can ensure that every LAN user accesses bandwidth fairly.
-------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

P2P Bandwidth Limits

- It determines the maximum bandwidth of P2P application.

Max. Bandwidth

- It determines the maximum bandwidth of the policy. (Note: The bandwidth is allocated to users that meet the criteria of the policy.)

New Sessions Per IP Per Second


- It determines the number of sessions that can be established per IP per second. Once the number of sessions exceeds the specified value, new sessions cannot be established.

Max. Concurrent Sessions Per IP

- It determines the maximum number of concurrent sessions of each IP address. If the amount of sessions exceeds the specified value, new sessions will not be created.

Max. Concurrent Sessions

- It determines the maximum number of concurrent sessions of a policy. If the amount of sessions exceeds the specified value, new sessions will not be created.

 Note	<p>Max. Concurrent Sessions overrides Max. Concurrent Sessions per IP in a policy. When the specified value of Max. Concurrent Sessions exceeds the one of Max. Concurrent Sessions per IP, the policy will apply the value of Max. Concurrent Sessions.</p>
---------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Traffic Quota per Session

- It determines the total traffic amount of a session. (KBytes)

Traffic Quota per Source IP

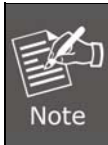
- It determines the quota of per source IP of a policy. (MBytes)

Traffic Quota per Day

- It determines the total traffic amount of a session per day. (MBytes)

IP Redirection

- There are three modes for WAN, LAN and DMZ:
 - ◆ Automatic: Automatically transferring the source IP address to the default IP address of MH-2300 device.
 - ◆ Routing: Delivering the packets using its original source IP and Destination IP.
 - ◆ NAT: Transferring the Source IP address to the designated IP address on the MH-2300 interface's subnet.



Under **Network > Interface**, the NAT Redirection, which is available for WAN interfaces, can be used for translating internal addresses into external addresses, whereas the **IP Redirection** (when selected as "NAT") of a network policy is to translate IP addresses from specific subnets.

Pause

- When modifications are required on existing settings, such as *Address* and *QoS*, you may temporarily disable the policy so as to modify the policy.

Priority

- When accessing packets, MH-2300 inspects the packet to see if it is identical with the criteria of existing policies. The packet-to-policy inspection is performed by the priority of policies. Therefore, in order to optimize the process, you may rearrange the priority of policies accordingly by changing the figure in the drop-down list of each policy.

6.1.1 Example

Prerequisite Configuration

Port1 is defined as LAN1 (192.168.1.1, NAT/ Routing mode) and is connected to the LAN: 192.168.1.X/24.

Port2 is defined as WAN1 (61.11.11.11) and is connected to the Internet via the ADSL modem (ATUR). (IP range: 61.11.11.10 to 61.11.11.14)

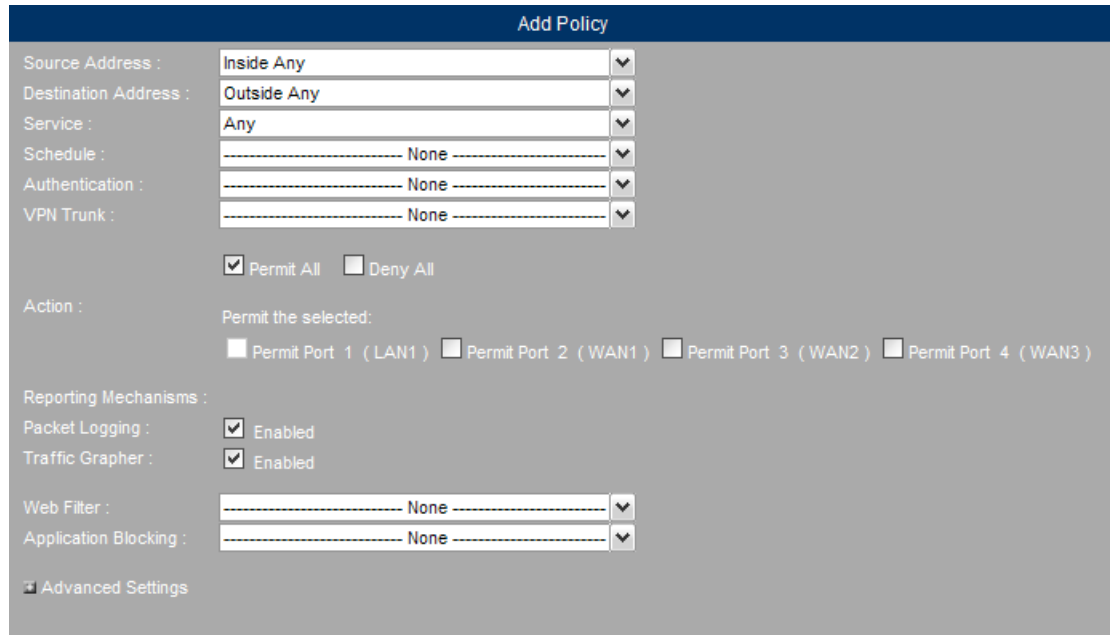
Port3 is defined as WAN2 (211.22.22.22) and is connected to the Internet via the ADSL modem (ATUR). (IP range: 211.22.22.18 to 211.22.22.30)

Port4 is defined as DMZ1.

6.1.1.1 Creating a Policy to Monitor the Internet Access of LAN Users (Using Packet Logging and Traffic Grapher)



Step 1. Go to **Policy > Outgoing** and then set as shown below:

- Enable the **Packet Logging**.
- Enable the **Traffic Grapher**.
- Click **OK**.



OK Cancel

Creating a Policy to Apply the Packet Logging and Traffic Grapher Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any			Modify Remove Pause	1

New Entry

Policy Successfully Created

Step 2. Click the **Packet Logging** icon  of a policy to see the log.

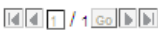
- On the upper-left corner, click the **Refresh** button or select a refresh interval from the drop-down list to obtain the up-to-date session information.
- Click any **Source IP** or **Destination IP** for sessions accessed through the IP address that you click on.
- For details of all sessions accessed through MH-2300, go to **Monitoring > Logs > Traffic** on the main menu.

manually

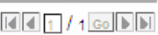
▼

Priority	Type	Source	Destination	Service	Action
1	Outgoing	Inside Any	Outside Any	Any	✓

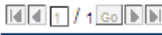
Outside Any



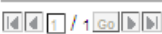
Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
19:28:29	192.168.1.2	192.168.99.1	UDP	63776→53(WAN=1)	57.0 B	✓
19:28:25	192.168.1.2	192.168.99.1	UDP	63776→53(WAN=1)	57.0 B	✓



The Packets Logged by a Policy



Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
19:28:29	192.168.1.2	192.168.99.1	UDP	63776→53(WAN=1)	57.0 B	✓
19:28:25	192.168.1.2	192.168.99.1	UDP	63776→53(WAN=1)	57.0 B	✓



Clear

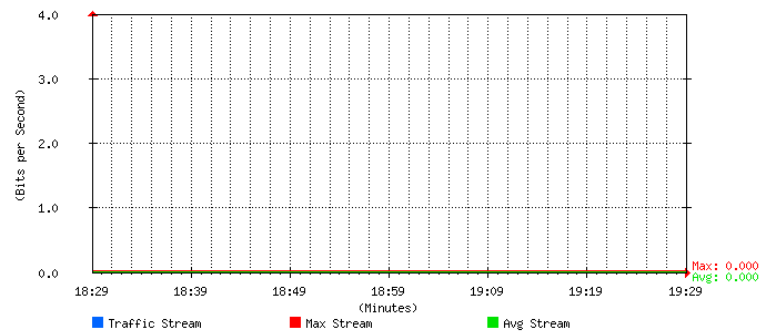
Packet Information Screen

Step 3. Under **Monitoring > Traffic Grapher > Policy-Based Traffic**, the traffic flow is displayed in graphics, giving you an instant insight into the traffic status.

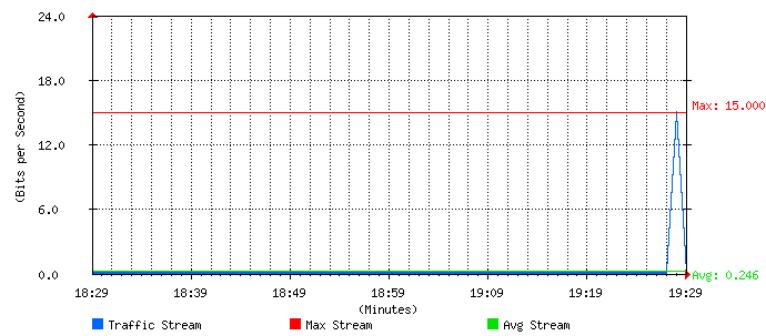
2010 / 12 / 24 19 : -- : --

Real-time: Down 0.0 Bits/sec Up 0.0 Bits/sec

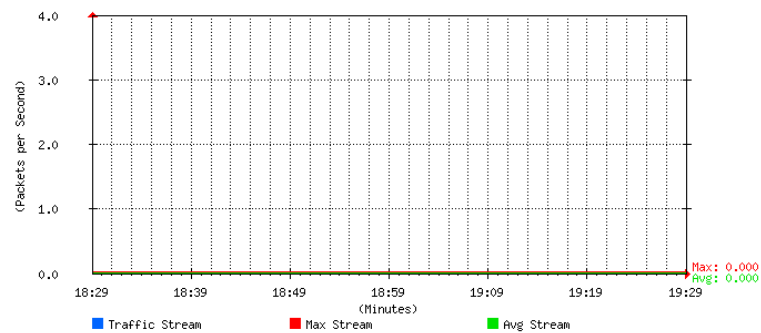
Downstream



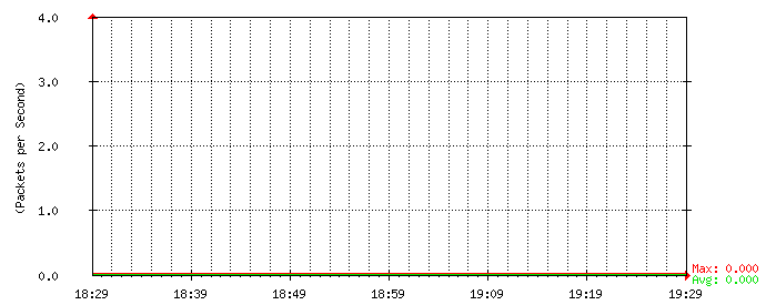
Upstream



Received Packets



Transmitted Packets



The Traffic Statistics Screen

6.1.1.2 Creating Policies to Restrict the Access to Specific Web Sites

Step 1. Go to **Web Filter > Configuration > Whitelist / Blacklist / File Extensions / MIME / Script / Group** and then set as shown below:

Export whitelist :

Import whitelist : (Max. file size: 1 MB)

Name ▲	URL ▲	File Access	Configuration
url_1	yahoo	✗	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
url_2	google	✗	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

1 / 1 Go

The Whitelist Rules for Allowing Website Access

Export blacklist :

Import blacklist : (Max. file size: 1 MB)

Name ▲	URL ▲	Configuration
url_3	*	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

1 / 1 Go

The Blacklist Rules for Blocking Website Access

Available File Extensions :

Name ▲	File Extension	Configuration
All_extend	exe, zip, rar, iso, bin...	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

1 / 1 Go

The File Extension Rules for Blocking File Transfers

Available MIME Types :

Name ▲	Forbidden Script Types	Forbidden MIME Types	Configuration
All_Script_MIME	Window Popup...	application/msword, application/octet-stream...	<input type="button" value="Modify"/>

1 / 1 Go

The MIME / Script Rule for Blocking Scripting Languages

Group Name ▲	Group Items	Configuration
Web_Blocking_Group	Whitelist : url1, url2 Blacklist : url3 Category : --- Upload Blocking : All_extend Download Blocking : All_extend MIME / Script : All_Script_MIME	<div>Modify Remove</div>

1 / 1 Go

New Entry

The Group Setting for Web Filtering Rules

Step 2. Go to **Policy Object > Application Blocking > Settings** and then set as shown below:

Add Application Blocking Rule

Rule Name : IM P2P Blocking (Max. 20 characters)

Instant Messenger Login (☒ Select All)

☒ MSN
☒ Yahoo
☒ ICQ/AIM
☒ QQ

☒ Skype
☒ Google Talk
☒ Gadu-Gadu
☒ Rediff

☒ WebIM
☒ AliSoft
☒ BaiduHi
☒ SinaUC

File Transfer over IM (☒ Select All)

☒ MSN
☒ Yahoo
☒ ICQ/AIM
☒ QQ

☒ Google Talk
☒ Gadu-Gadu

Peer-to-Peer Sharing (☒ Select All)

☒ Edonkey/eMule
☒ Bit Torrent/BitConnect
☒ WinMX
☒ Foxy

☒ KuGoo
☒ AppleJuice
☒ AudioGalaxy
☒ DirectConnect

☒ iMesh
☒ MUTE
☒ Thunder5
☒ GoGoBox

☒ QQDownload
☒ Ares
☒ Shareaza
☒ BearShare

☒ Morpheus
☒ Limewire
☒ KaZaa

Multimedia Streaming

Web-Based Mail

Online Gaming

VPN Tunneling

Remote Controlling

Other Application

OK Cancel

Creating an Application Blocking Rule

Application Signatures Settings

Last updated on : 2010/12/24 19:00:03 (Signatures updated hourly)

Current version : 6.3.4 (Updated at 2010/12/24 16:00:14)


Manually update signatures (Using TCP port: 80 and UDP port: 53) [Update Now](#) [Test Connection](#)

Application Blocking Rules

Rule Name ▲	Application	Configuration
IM P2P Blocking	MSN, Yahoo, ICQ/AIM, QQ, Skype, Google Talk, Gadu-Gadu, Rediff, W...	Modify Remove

[New Entry](#)

Application Blocking Rule Successfully Created



Note

- Web Filter** is intended for blocking the access to specific websites, scripting languages (e.g., the Java and cookies used on a stock exchange website), or HTTP / FTP file transfers.
- Application Blocking** is intended for blocking the use of instant messaging, peer-to-peer sharing, video / audio streaming, Web-based email messaging, online gaming, VPN tunneling, remote controlling and other applications.

Go to **Policy Object > Address > WAN / WAN Group** and then set as shown below:

Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 1 MB)

Name ▲	IP Version	IP Address / Netmask	Configuration
Outside Any	---	---	In Use
Remote_Server1	IPv4	61.219.38.98 / 255.255.255.255	Modify Remove
Remote_Server2	IPv4	202.1.237.21 / 255.255.255.255	Modify Remove

[New Entry](#)

The Address Settings for the Remote Servers

Name ▲	Group Members	Configuration
*CHU	---	In Use Remove
*CHINA_TELECOM	---	In Use Remove
WAN_GROUP	Remote_Server1, Remote_Server2	Modify Remove

*CHINA_TELECOM AND *CHU [Help](#)

[New Entry](#)

The Group Setting for WAN Addresses

Step 3. Go to **Policy > Outgoing** and then set as shown below:

- Click **New Entry**.
- Select the defined group from the **Destination Address** field.
- Select **Deny all outgoing connections** for **Action**.
- Click **OK**.

Add Policy

Source Address :	<div style="border: 1px solid #ccc; padding: 2px;">Inside Any</div> ▼
Destination Address :	<div style="border: 1px solid #ccc; padding: 2px;">WAN_GROUP</div> ▼
Service :	<div style="border: 1px solid #ccc; padding: 2px;">Any</div> ▼
Schedule :	<div style="border: 1px solid #ccc; padding: 2px;">----- None -----</div> ▼
Authentication :	<div style="border: 1px solid #ccc; padding: 2px;">----- None -----</div> ▼
VPN Trunk :	<div style="border: 1px solid #ccc; padding: 2px;">----- None -----</div> ▼

☐ Permit All ☒ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (DMZ1)
 ☐ Permit Port 4 (WAN2)

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

----- None -----

 ▼

Application Blocking :

----- None -----

 ▼

Advanced Settings

OK

Cancel

Creating a Policy for Denying All Outgoing Connections

Step 4. Go to **Policy > Outgoing** and then set as shown below:

- Click **New Entry**.
- Select the defined group from the **Web Filter** drop-down list.
- Select the defined rule from the **Application Blocking** drop-down list.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼
Destination Address : Outside Any ▼
Service : Any ▼
Schedule : ----- None ----- ▼
Authentication : ----- None ----- ▼
VPN Trunk : ----- None ----- ▼

☒ Permit All ☐ Deny All

Action : Permit the selected:
☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (DMZ1) ☐ Permit Port 4 (WAN2)

Reporting Mechanisms :
Packet Logging : ☐ Enabled
Traffic Grapher : ☐ Enabled

Web Filter : Web_Blocking_Group ▼
Application Blocking : IM P2P Blocking ▼

☐ Advanced Settings

Creating a Policy to Apply the Web Filtering and Application Blocking Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	WAN_GROUP	Any	✗		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	1 ▼
Inside Any	Outside Any	Any	✓	🚫	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	2 ▼

 1 / 1

New Entry

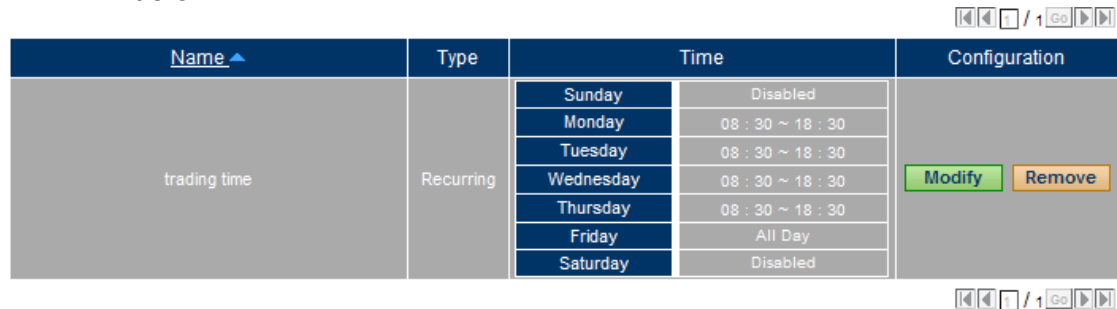
Policy Successfully Created

Note

The **Deny ALL** feature of a policy can block the packets that meet the criteria. The IT administrator can adjust the order of this policy to the first rank so as to stop LAN users from accessing specific IP address.

6.1.1.3 Creating a Policy to Grant Internet Access to Only Authenticated Users on Schedule

Step 1. Go to **Policy Object > Schedule > Settings** and then set as shown below:

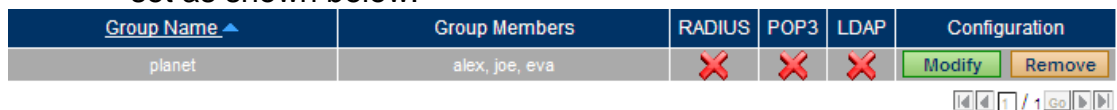


Name ▲	Type	Time	Configuration														
trading time	Recurring	<table border="1"> <tr><td>Sunday</td><td>Disabled</td></tr> <tr><td>Monday</td><td>08 : 30 ~ 18 : 30</td></tr> <tr><td>Tuesday</td><td>08 : 30 ~ 18 : 30</td></tr> <tr><td>Wednesday</td><td>08 : 30 ~ 18 : 30</td></tr> <tr><td>Thursday</td><td>08 : 30 ~ 18 : 30</td></tr> <tr><td>Friday</td><td>All Day</td></tr> <tr><td>Saturday</td><td>Disabled</td></tr> </table>	Sunday	Disabled	Monday	08 : 30 ~ 18 : 30	Tuesday	08 : 30 ~ 18 : 30	Wednesday	08 : 30 ~ 18 : 30	Thursday	08 : 30 ~ 18 : 30	Friday	All Day	Saturday	Disabled	<div>Modify Remove</div>
Sunday	Disabled																
Monday	08 : 30 ~ 18 : 30																
Tuesday	08 : 30 ~ 18 : 30																
Wednesday	08 : 30 ~ 18 : 30																
Thursday	08 : 30 ~ 18 : 30																
Friday	All Day																
Saturday	Disabled																

New Entry

Figure 16-18 The Schedule Setting for Internet Access

Step 2. Go to **Policy Object > Authentication > Account / Group** and then set as shown below:



Group Name ▲	Group Members	RADIUS	POP3	LDAP	Configuration
planet	alex, joe, eva	✗	✗	✗	<div>Modify Remove</div>

New Entry

The Group Setting for User Authentication

Step 3. Go to **Policy > Outgoing** and then set as shown below:

- Select the defined group from the **Authentication** drop-down list.
- Select the defined rule from the **Schedule** drop-down list.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼
Destination Address : Outside Any ▼
Service : Any ▼
Schedule : trading time ▼
Authentication : planet ▼
VPN Trunk : ----- None ----- ▼

☒ Permit All ☐ Deny All

Action : Permit the selected:
☐ Permit Port 1 (LAN1) ☐ Permit Port 2 (WAN1) ☐ Permit Port 3 (DMZ1) ☐ Permit Port 4 (WAN2)

Reporting Mechanisms :
Packet Logging : ☐ Enabled
Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼
Application Blocking : ----- None ----- ▼

[⚙ Advanced Settings](#)

OK
Cancel

Creating a Policy to Apply the Schedule and Authentication Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✔🕒🔒		Modify Remove Pause	1 ▼

🔍 📄 🏠 / 1 Go 🔍

New Entry

Policy Successfully Created

6.1.1.4 Creating a Policy to Enable a Remote User to Control a LAN PC by Remote Control Software (pcAnywhere)

Step 1. Set up a computer to be remotely controlled; its IP address is 192.168.1.2.

Step 2. Under **Policy Object > Virtual Server > Port Mapping**, set as shown below:

Name ▲	Public IP Address	Service	Private IP Address #	Configuration
Remote_Control	61.11.11.12 Port2 (WAN1)	PC-Anywhere	192.168.1.2 (LAN)	Modify Remove

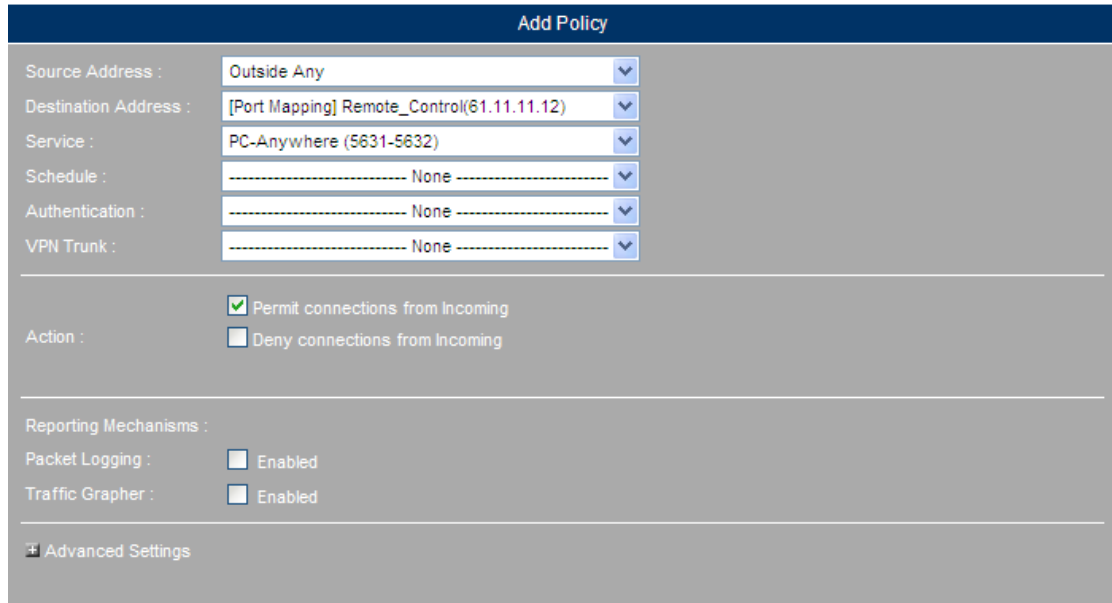
🔍 📄 🏠 / 1 Go 🔍

New Entry

The Mapping Rule for the Remote Controlling

Step 3. Under **Policy > Incoming**, set as shown below:

- Select the defined Virtual Server for **Destination Address**.
- Select "PC-Anywhere(5617-5632)" for **Service**.
- Click **OK**.



OK Cancel

Creating a Policy for External Users Controlling an Internal PC Remotely

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](61.11.11....	PC-Anywh...	✓		Modify Remove Pause	1

1 / 1 Go

New Entry

Policy Successfully Created

6.1.1.5 Creating a Policy to Limit the Downloaded Bandwidth, Daily Traffic Quota and Maximum Concurrent Sessions of FTP Service (Running FTP Server in DMZ in NAT Mode)

Step 1. Set up an FTP server in DMZ with an IP address of 192.168.3.2. (The DMZ subnet is set to 192.168.3.1/24.)

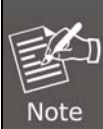
Step 2. Under **Policy Object > Virtual Server > Port Mapping**, set as shown below:

Name	Public IP Address	Service	Private IP Address #	Configuration
FTP_Server	61.11.11.12 Port2 (WAN1)	FTP	192.168.3.2 (DMZ)	Modify Remove

1 / 1 Go

New Entry

The Mapping Rule for the FTP Server



Note

To avoid exposing your networks to hackers, it is strongly recommended not to select "ANY" for **Service** when configuring an incoming policy or WAN-to-DMZ policy.

Step 3. Go to **Policy Object > QoS > Settings** and then set as shown below:

Name ▲	Interface	Downstream Bandwidth	Upstream Bandwidth	Priority	Configuration
Policy Qos	1 (LAN1)	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	Medium	<div>Modify</div> <div>Remove</div>
	2 (WAN1)	G.Bandwidth = 100 Kbps M.Bandwidth = 500 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 200 Kbps		
	3 (DMZ1)	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		
	4 (WAN2)	G.Bandwidth = 500 Kbps M.Bandwidth = 512 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 60 Kbps		

1 / 1 Go

New Entry

The QoS Setting for the FTP Service

Step 4. Go to **Policy > WAN to DMZ** and then set as shown below

- Select the defined rule from the **Destination Address** drop-down list.
- Select "FTP(24-21)" from the **Service** drop-down list.
- Select the defined rule from the **QoS** drop-down list.
- Enter "100" in the **Max. Concurrent Sessions** field.
- Type "100000" in the **Traffic Quota Per Day** field.
- Click **OK**.

Add Policy

Source Address : Outside Any ▼

Destination Address : [Port Mapping] FTP_Server(61.11.11.12) ▼

Service : FTP (20-21) ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : ----- None ----- ▼

Action : ☒ Permit connections from WAN to DMZ
☐ Deny connections from WAN to DMZ

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

⊟ Advanced Settings

IDP : ☐ Enabled

Anti-Virus : ☐ POP3 ☐ SMTP

Anti-Spam : ☐ POP3 ☐ SMTP

QoS : Policy Qos ▼

Max. Bandwidth Per Source IP : Downstream 0 Kbps / Upstream 0 Kbps (0: unlimited)

Max. Concurrent Sessions Per IP : 0 (1 - 99999, 0: unlimited)

Max. Concurrent Sessions : 100 (1 - 99999, 0: unlimited)

Traffic Quota per Session : 100000 KB (1 - 999999, 0: unlimited)

Quota Per Source IP : 0 MB (1 - 999999, 0: unlimited)

Traffic Quota per Day : 0 MB (1 - 999999, 0: unlimited)

IP Redirection :

Port 1 (LAN1) :	Automatic ▼	
Port 2 (WAN1) :	Automatic ▼	
Port 3 (DMZ1) :	Automatic ▼	
Port 4 (WAN2) :	Automatic ▼	

Help

Creating a Policy for External Users Accessing FTP Server

Source	Destination	Service	Action	Options	Configuration	Priority
Outside Any	[Port Mapping](61.11.11....	FTP	✓		Modify Remove Pause	1



[New Entry](#)

Policy Successfully Created

6.1.1.6 Creating Policies to Enable LAN / WAN Users to Have Email Access (Running Mail Server in DMZ in Transparent Mode)

Step 1. Set up a mail server in DMZ with an IP address of 61.11.11.12 and resolve the domain name with an external DNS server.

Step 2. Under **Policy Object > Address > DMZ**, set as shown below:

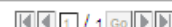
Export data entries : [Export](#)

Import data entries : [Browse...](#) [Import](#) (Max. file size: 1 MB)

[Assist Me](#)



Name ▲	IP Version	Interface	IP Address / Netmask	MAC Address	Configuration
DMZ Any	---	All	---		In Use
Mail_Server	IPv4	All	61.11.11.12 / 255.255.255.255		Modify

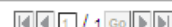


[New Entry](#)

The Address Setting for the DMZ Mail Server

Step 3. Under **Policy Object > Service > Group**, set as shown below:

Group Name ▲	Group Items	Configuration
Email	DNS, POP3, SMTP	Modify Remove



[New Entry](#)

The Group Setting for Email Service

Step 4. Under **Policy > WAN To DMZ**, set as shown below:

- Select the predefined address rule for **Destination Address**.
- Select the predefined service rule for **Service**.
- Click **OK**.

Add Policy

Source Address :

Outside Any

Destination Address :

Mail_Server

Service :

Email

Schedule :

----- None -----

Authentication :

----- None -----

VPN Trunk :

----- None -----

☒ Permit connections from WAN to DMZ

☐ Deny connections from WAN to DMZ

Reporting Mechanisms :

Packet Logging :
☐ Enabled

Traffic Grapher :
☐ Enabled

⚙ Advanced Settings

OK

Cancel

Creating a Policy for External Users Accessing DMZ Mail Server

Source	Destination	Service	Action	Options					Configuration			Priority
Outside Any	Mail_Server	Email	✔						Modify	Remove	Pause	1

⏮ ⏪ ⏩ ⏭ / 1 ⏮ ⏭ ⏩ ⏭

New Entry

Policy Successfully Created

Step 5. Under **Policy > LAN To DMZ**, set as shown below:

- Select the predefined address rule for **Destination Address**.
- Select the predefined service rule for **Service**.
- Click **OK**.

Add Policy

Source Address : Inside Any ▼

Destination Address : Mail_Server ▼

Service : Email ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

Action : ☒ Permit connections from LAN to DMZ
☐ Deny connections from LAN to DMZ

Reporting Mechanisms :

Packet Logging : ☐ Enabled

Traffic Grapher : ☐ Enabled

Advanced Settings

OK
Cancel

Creating a Policy for Internal Users Accessing DMZ Mail Server

Source	Destination	Service	Action	Options				Configuration			Priority
Inside Any	Mail_Server	Email	✓					Modify	Remove	Pause	1 ▼

1 / 1

New Entry

Policy Successfully Created

Step 6. Under **Policy > DMZ To WAN**, set as shown below:

- Select the predefined address rule for **Source Address**.
- Select the predefined service rule for **Service**.
- Click **OK**.

Add Policy

Source Address : Mail_Server ▼

Destination Address : Outside Any ▼

Service : Email ▼

Schedule : ----- None ----- ▼

Authentication : ----- None ----- ▼

VPN Trunk : ----- None ----- ▼

☒ Permit All
 ☐ Deny All

Action : Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (WAN1)
 ☐ Permit Port 3 (DMZ1)
 ☐ Permit Port 4 (WAN2)

Reporting Mechanisms :

Packet Logging : ☐ Enabled
 Traffic Grapher : ☐ Enabled

Web Filter : ----- None ----- ▼

Application Blocking : ----- None ----- ▼

Advanced Settings

OK

Cancel

Creating a Policy for External Users Accessing the DMZ Mail Server

Source	Destination	Service	Action	Options								Configuration			Priority
Mail_Server	Outside Any	Email	✔									Modify	Remove	Pause	1 ▼

New Entry

Policy Successfully Created

Chapter 7. Abnormal IP Flow

7.1 Abnormal IP Flow

Once an abnormal traffic flow is detected, MH-2300 will take action to block the flow of packets. This protection ensures that the network remains operational, and consequently the business revenue generating opportunities are left undisturbed.

7.1.1 Example

7.1.1.1 Configuring the Alert Notification for Abnormal IP Flow and Blocking the DDoS Attack from the Infected Devices

Step 1. Go to **System > Configuration > Settings** and then configure the settings under the **Email Notification Settings** section.

Step 2. Go to **Anomaly Flow IP > Settings** and then set as shown below:

- Enter the **Traffic Threshold per IP**. (The default value is 100)
- Tick **Enable Anomaly Flow IP Blocking** and then type the **Blocking Time**. (The default value is 60)
- Tick **Enable E-Mail Alert Notification**.
- Tick **Enable SNMP traps**.
- Tick **Enable NetBIOS notification** and then type the **Administrator's IP Address**.
- Click **OK**.

Anomaly Flow IP Settings

Traffic Threshold per IP sessions / sec (1 - 9999)

☒ Enable Anomaly Flow IP Blocking Blocking Time second(s) (1 - 999)

☒ Enable E-Mail Alert Notification

Anomaly Traffic User Warning Message [Preview](#)

```

It might be affected by the virus.
<BR>
Please contact your onsite IT administrator for assistance.
</b>
</font>
</form>
</center>
</body>


```

DoS / Anti-Attack Setting

<input type="checkbox"/> Sasser Block	<input type="checkbox"/> MSBlaster Block
<input type="checkbox"/> Code Red Block	<input type="checkbox"/> Nimda Block
<input type="checkbox"/> Detect SYN Attack	SYN Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec
	SYN Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec
	SYN Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Second(s)
<input type="checkbox"/> Detect ICMP Attack	ICMP Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec
	ICMP Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec
	ICMP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Second(s)
<input type="checkbox"/> Detect UDP Attack	UDP Flood Threshold (Total) <input type="text" value="0"/> Pkts/Sec
	UDP Flood Threshold (Per Source IP) <input type="text" value="0"/> Pkts/Sec
	UDP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="0"/> Second(s)
<input type="checkbox"/> Detect Ping of Death Attack	<input type="checkbox"/> Detect Tear Drop Attack
<input type="checkbox"/> Detect IP Spoofing Attack	<input type="checkbox"/> Filter IP Route Option
<input type="checkbox"/> Detect Port Scan Attack	<input type="checkbox"/> Detect Land Attack

Detection-Excluded IP			
Interface ▲	IP Version ▲	IP Address ▲	Configuration
No data found !			

Anomaly Flow IP Settings

- 

1. **Detection-excluded IP** can be used for excluding specific IPs from detection.

2. Users whose PCs emit abnormal traffic flows can receive a customizable message in their browser to alert them about the incident.

Step 3. When a DDoS attack occurs, MH-2300 generates a corresponding log under **Anomaly Flow IP > Virus-infected IP**.

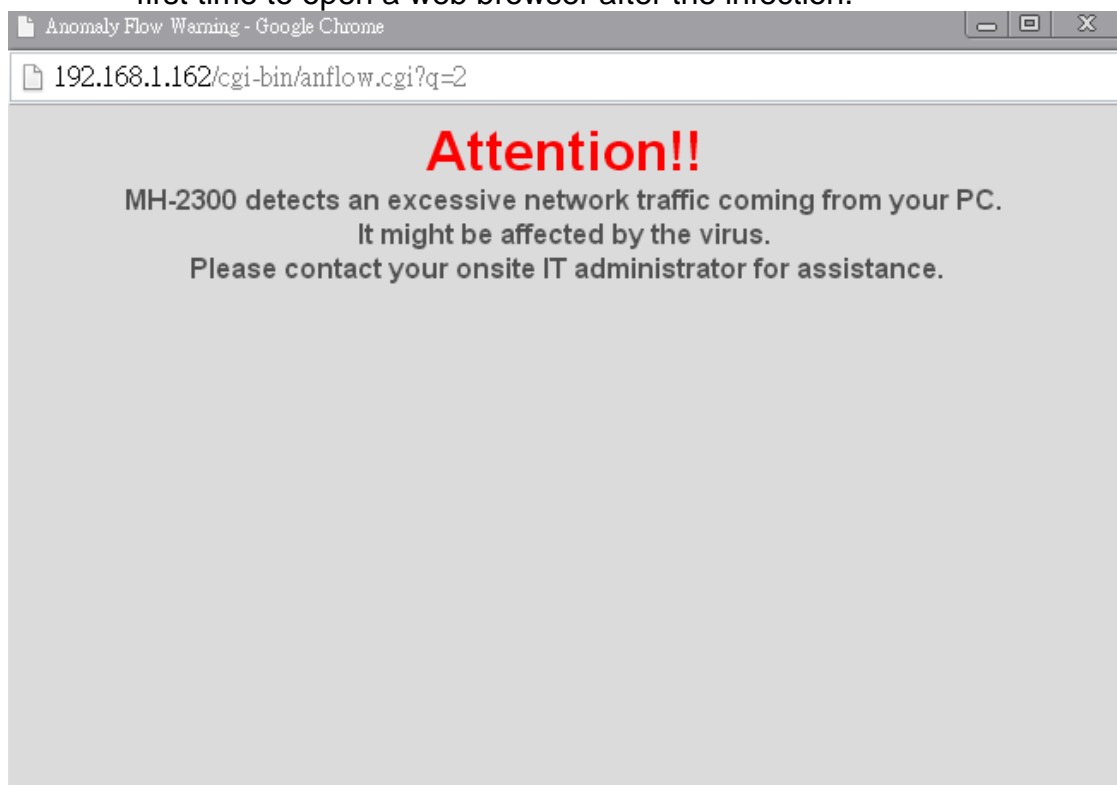
Traffic Threshold per IP : 100 sessions / sec

Interface	Protocol	Virus-Infected IP	MAC Address	Alarm Time ▼
LAN	IPv4	FILE-SERVER	A8:F7:E0:11:22:33	2014-12-16 10:35:04

The Virus-Infected IP Address Table

Step 4. The alert notification sent to the designated recipient.

Step 5. Internal virus-infected users will see an alert message upon opening a web browser. MH-2300 limits virus-infected users' bandwidth to a minimum in order to oblige users to take action to remove virus. Note: The alert message merely appears to virus-infected users at the very first time to open a web browser after the infection.



An Alert Message Shown to a Virus-Infected User

Chapter 8. Monitoring

8.1 Logs

Log comprises logs of Traffic, Events, Connections, Viruses, Application Blocking, Concurrent Sessions and Quota. The system may send the logs to the IT administrator automatically or back up the logs to a remote device.

- Traffic Logs can be enabled under **Policy**, the sessions of the Policy will be recorded in detail.
- Event Logs have the records of any system configurations made. Each log denotes who, when, what and where that a configuration is being modified.
- Connection Logs comprehensively record all connection related data, such as VPN, PPPoE, SMTP, POP3, etc., providing the IT administrator with an instant insight when any connection issues arise.
- Application Blocking Logs provide details of all the applications that have been blocked by the MH-2300.
- Concurrent Sessions Logs provide details of the Max. Concurrent Sessions of each policy.
- Quota Logs provide details of the quota of each policy.

Terms in Settings

Logging Settings

- Logs are sent to the designated recipient once the file size reaches 300 KB.
- Logs can be backed up onto the remote device.
- The log setting of traffic, events, connections, application blocking, concurrent sessions and traffic quota:
 - ◆ You may enable email logs, syslog messages, RSS feeds, accordingly.

8.1.1 Traffic

8.1.1.1 Viewing the Logs of Used Protocols and Port Numbers

Step 1. Go to **Policy> DMZ To WAN** and set as shown below:

- Enable the **Packet Logging**.
- Click **OK**.

Add Policy

Source Address :

DMZ Any

Destination Address :

Outside Any

Service :

Any

Schedule :

----- None -----

Authentication :

----- None -----

VPN Trunk :

----- None -----

☒ Permit All ☐ Deny All

Action :

Permit the selected:

☐ Permit Port 1 (LAN1)
 ☐ Permit Port 2 (DMZ1)
 ☐ Permit Port 3 (WAN2)
 ☐ Permit Port 4 (WAN3)

Reporting Mechanisms :

Packet Logging : ☒ Enabled

Traffic Grapher : ☐ Enabled

Web Filter :

----- None -----

Application Blocking :

----- None -----

Advanced Settings

OK

Cancel

Creating a Policy to Enable Packet Logging for DMZ Traffic

Source	Destination	Service	Action	Options	Configuration	Priority
DMZ Any	Outside Any	Any			<div>Modify</div> <div>Remove</div> <div>Pause</div>	1

New Entry

Policy Successfully Created

Step 2. Under **Monitoring > Logs > Traffic**, it shows the traffic status of a policy.

- Click any **Source IP** or **Destination IP**, you will see of which protocols and ports it used and its traffic.
- To clear the logs, click the **Clear** button and then click **OK** in the confirmation window.

Refresh


1 / 31 Go

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
18:53:14	192.168.1.2	119.161.9.232	TCP	50590→80(WAN=3)	1.5 KB	✓
18:53:12	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:53:10	192.168.2.22	218.61.6.152	UDP	5041→8007(WAN=3)	135.0 B	✓
18:53:09	192.168.1.2	180.233.118.157	TCP	50589→1935(WAN=2)	231.2 KB	✓
18:53:08	192.168.1.2	67.195.133.149	TCP	50587→80(WAN=2)	2.8 KB	✓
18:53:08	192.168.1.2	119.161.9.232	TCP	50588→80(WAN=2)	1.5 KB	✓
18:53:02	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:52:52	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
18:52:50	192.168.2.22	119.167.215.53	UDP	5041→8003(WAN=3)	135.0 B	✓
18:52:48	192.168.1.2	203.84.204.124	TCP	50586→80(WAN=3)	1.5 KB	✓
18:52:48	192.168.1.2	119.160.246.14	TCP	50585→80(WAN=3)	30.9 KB	✓
18:52:46	192.168.1.2	61.213.183.97	TCP	50584→80(WAN=3)	4.3 KB	✓
18:52:45	192.168.1.2	72.30.14.127	TCP	50582→80(WAN=2)	1.6 KB	✓
18:52:45	192.168.1.2	203.84.196.149	TCP	50583→80(WAN=2)	3.0 MB	✓
18:52:44	192.168.1.2	67.195.160.33	TCP	50580→80(WAN=3)	1.5 KB	✓
18:52:44	192.168.1.2	203.69.138.19	TCP	50581→80(WAN=3)	42.9 KB	✓
18:52:43	192.168.1.2	203.84.204.124	TCP	50577→80(WAN=3)	1.7 KB	✓
18:52:43	192.168.1.2	124.108.78.87	TCP	50574→80(WAN=2)	4.8 KB	✓
18:52:43	192.168.1.2	124.108.103.68	TCP	50579→80(WAN=3)	5.5 KB	✓
18:52:43	192.168.1.2	124.108.103.68	TCP	50576→80(WAN=3)	8.1 KB	✓

1 / 31 Go

Clear

The Traffic Logs

Refresh

1 / 51 Go

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
19:08:33	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:08:30	192.168.2.22	218.61.6.150	UDP	5041→8004(WAN=2)	135.0 B	✓
19:08:23	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:08:13	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:08:10	192.168.2.22	220.165.14.16	UDP	5041→8000(WAN=2)	135.0 B	✓
19:08:10	192.168.2.22	218.61.6.152	UDP	5041→8007(WAN=2)	135.0 B	✓
19:08:03	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:07:53	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:07:43	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:07:33	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:07:30	192.168.2.22	218.61.6.150	UDP	5041→8004(WAN=3)	135.0 B	✓
19:07:23	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:07:13	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:07:10	192.168.2.22	218.61.6.152	UDP	5041→8007(WAN=3)	135.0 B	✓
19:07:10	192.168.2.22	119.160.245.215	TCP	2705→80(WAN=3)	1.6 KB	✓
19:07:05	192.168.2.22	119.160.246.241	TCP	2703→80(WAN=2)	1.9 KB	✓
19:07:03	192.168.2.22	119.160.246.241	TCP	2701→80(WAN=2)	2.0 KB	✓
19:07:03	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=2)	42.0 B	✓
19:07:01	192.168.2.22	119.160.246.241	TCP	2699→80(WAN=2)	2.0 KB	✓
19:06:59	192.168.2.22	120.29.145.26	TCP	2697→80(WAN=3)	22.0 KB	✓

1 / 51 Go

Clear

The Traffic Logs of a Specific IP Address

Refresh

1 / 55 Go

Time	Source IP	Destination IP	Protocol	Port	Traffic	Disposition
19:10:23	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:10:20	192.168.1.2	119.161.9.232	TCP	50848→80(WAN=3)	1.5 KB	✓
19:10:16	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=2)	7.8 KB	✓
19:10:16	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:16	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:15	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:15	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:15	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:15	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:15	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	7.8 KB	✓
19:10:14	192.168.1.2	111.221.16.219	TCP	50847→443(WAN=3)	48.0 B	✓
19:10:13	192.168.2.22	118.123.212.13	UDP	5041→7000(WAN=3)	42.0 B	✓
19:10:13	192.168.1.2	119.161.9.232	TCP	50837→80(WAN=2)	1.5 KB	✓
19:10:10	192.168.2.22	220.165.14.16	UDP	5041→8000(WAN=3)	135.0 B	✓
19:10:10	192.168.2.22	218.61.6.152	UDP	5041→8007(WAN=3)	135.0 B	✓
19:10:08	192.168.1.2	119.161.9.232	TCP	50835→80(WAN=3)	52.0 B	✓
19:10:05	192.168.1.2	203.84.204.124	TCP	50834→80(WAN=3)	1.5 KB	✓
19:10:05	192.168.1.2	119.161.9.232	TCP	50835→80(WAN=3)	52.0 B	✓
19:10:05	192.168.1.2	119.160.244.10	TCP	50833→80(WAN=2)	2.0 KB	✓
19:10:04	192.168.1.2	192.168.0.1	TCP	50832→80(WAN=2)	52.0 B	✓

1 / 55 Go

Clear

Deleting All the Traffic Logs

8.1.2 Events

8.1.2.1 Viewing the System Events and WAN Status

Step 1. Under **Monitoring > Logs > Events**, there it shows the system history access and the status of WAN.

[Refresh](#)

2010-12-22 (39 records) ▼

1 / 2 Go

Time ▼	Admin Name ▼	IP Address ▼	Event ▼	Details ▼
19:10:14	admin	192.168.1.2	Login successful.	---
18:40:17	admin	211.75.117.114	[Policy→DMZ to WAN] Setting(s) added.	📁
18:38:48	admin	211.75.117.114	[Network→Interface] Setting(s) modified.	📁
18:38:30	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	📁
18:38:26	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	📁
18:37:51	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	📁
18:37:47	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	📁
18:36:29	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) removed.	📁
18:22:04	admin	211.75.117.114	[Policy→Outgoing] Setting(s) modified.	📁
18:04:38	admin	211.75.117.114	[Policy→Incoming] Setting(s) removed.	📁
18:04:25	admin	211.75.117.114	Login successful.	---
18:04:25	admin	211.75.117.114	[Policy→Incoming] Setting(s) added.	📁
18:04:07	admin	211.75.117.114	[Policy→Incoming] Setting(s) added.	📁
17:56:05	admin	211.75.117.114	Login successful.	---
17:56:03	admin	211.75.117.114	Login successful.	---
17:56:02	admin	211.75.117.114	Login successful.	---
17:55:51	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) added.	📁
17:54:02	admin	211.75.117.114	[Policy Object→Virtual Server→Port Mapping] Setting(s) added.	📁
16:45:27	admin	211.75.117.114	[Policy Object→Application Blocking→Settings] Setting(s) added.	📁
16:33:46	admin	211.75.117.114	[Policy Object→Application Blocking→Settings] Setting(s) added.	📁

1 / 2 Go

The Event Logs

8.1.3 Connections

8.1.3.1 Viewing the Logs of WAN Connectivity

Step 1. Under **Monitoring > Logs > Connections**, it shows the logs of PPPoE, Dynamic IP Address, DHCP, PPTP Server, PPTP Client, IPsec and Web VPN.

- To delete the logs, click the **Clear** button and then click **OK** in the confirmation window.

Connection type : PPPoE
2010-12-22(2608 recorders)

1 / 131



Time	Connection
18:38:46	recv (receivePacket)
18:38:36	pppd 2.4.4 started by root, uid 0
18:38:36	RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
18:38:36	Plugin /usr/lib/pppd/2.4.4/rp-pppoe.so loaded.
18:38:10	Exit.
18:38:10	Unable to complete PPPoE Discovery
18:38:10	Timeout waiting for PADO packets
18:37:35	pppd 2.4.4 started by root, uid 0
18:37:35	RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
18:37:35	Plugin /usr/lib/pppd/2.4.4/rp-pppoe.so loaded.
18:37:09	Exit.
18:37:09	Unable to complete PPPoE Discovery
18:37:09	Timeout waiting for PADO packets
18:36:34	pppd 2.4.4 started by root, uid 0
18:36:34	RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
18:36:34	Plugin /usr/lib/pppd/2.4.4/rp-pppoe.so loaded.
18:36:09	Exit.
18:36:09	Unable to complete PPPoE Discovery
18:36:09	Timeout waiting for PADO packets
18:35:34	pppd 2.4.4 started by root, uid 0

1 / 131



The Connection Logs

Refresh

Connection type : PPPoE 2010-12-22(2608 recorders)

 1 / 131 **Go** 

Time	Connection
18:38:46	recv (receivePacket)
18:38:36	pppd 2.4.4 started by root, uid 0
18:38:36	RP-PPPoE p
18:38:36	Plugin /usr/li
18:38:10	Exit.
18:38:10	Unable to co
18:38:10	Timeout wa
18:37:35	pppd 2.4.4 s
18:37:35	RP-PPPoE p
18:37:35	Plugin /usr/li
18:37:09	Exit.
18:37:09	Unable to complete PPPoE Discovery
18:37:09	Timeout waiting for PADO packets
18:36:34	pppd 2.4.4 started by root, uid 0
18:36:34	RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
18:36:34	Plugin /usr/lib/pppd/2.4.4/rp-pppoe.so loaded.
18:36:09	Exit.
18:36:09	Unable to complete PPPoE Discovery
18:36:09	Timeout waiting for PADO packets
18:35:34	pppd 2.4.4 started by root, uid 0

 1 / 131 **Go** 

Clear

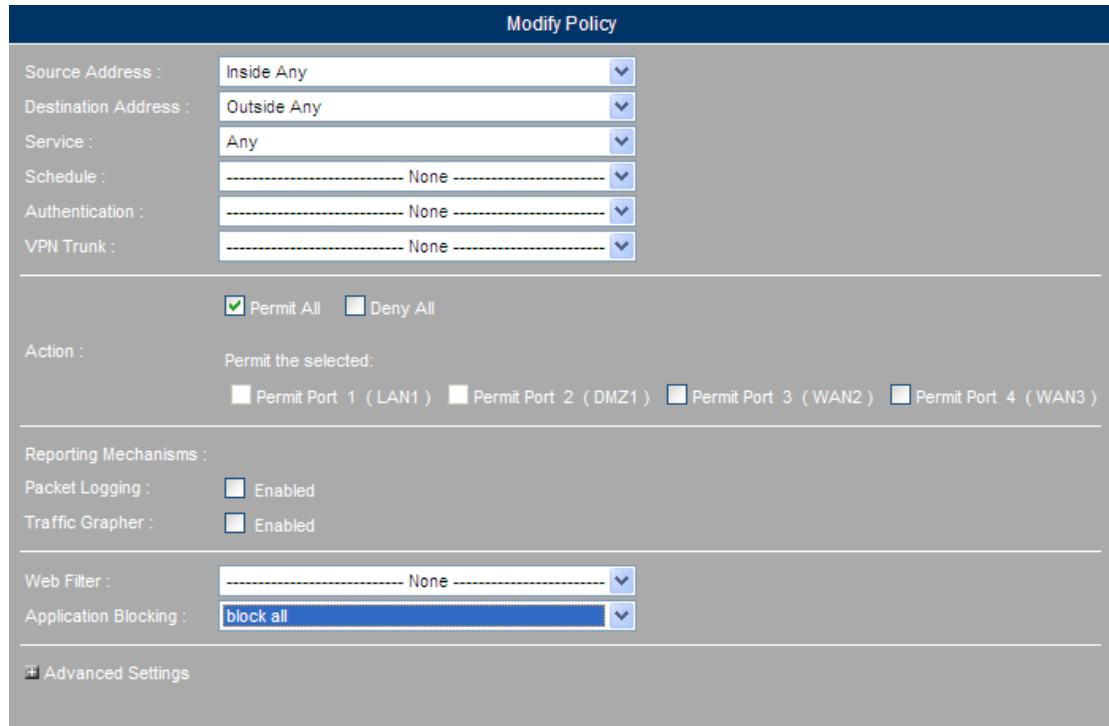
Deleting All the Connection Logs

8.1.4 Application Blocking

8.1.4.1 Viewing the Logs of IPs That Attempted to Access Restricted Applications




Step 1. Under **Policy > Outgoing**, set as shown below:

- Select the defined application blocking.
- Click **OK**.



OK **Cancel**

Creating a Policy to Apply the Application Blocking Settings

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any			Modify Remove Pause	1 




New Entry


Policy Successfully Created

Step 2. Under **Monitoring > Logs > Application Blocking**, it shows the logs of applications that have been blocked.

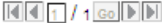
- To delete the logs, click the **Clear** button and then click **OK** from the confirmation window.

Refresh

2010-12-22 (1 Record) 

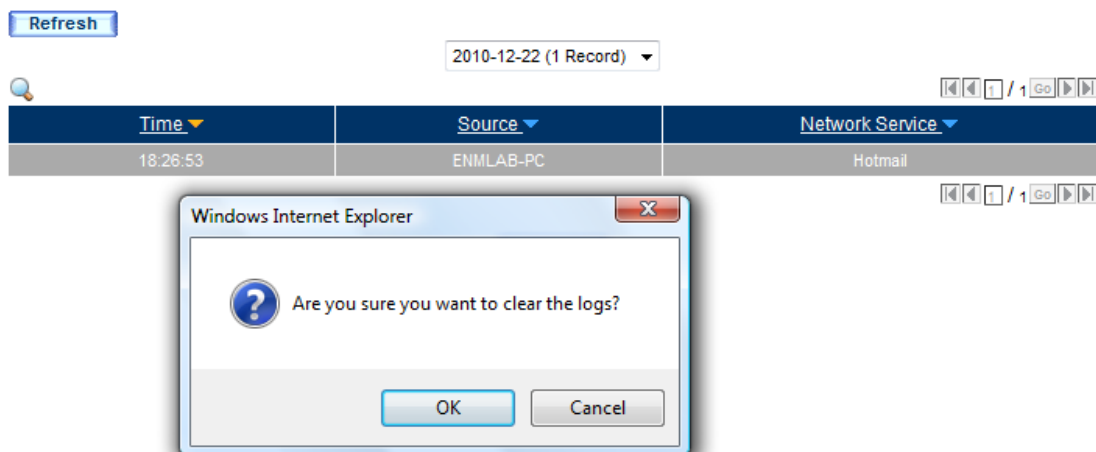


Time	Source	Network Service
18:26:53	ENMLAB-PC	Hotmail



Clear

The Application Blocking Logs



Deleting the Application Blocking Logs

8.1.5 Concurrent Sessions

8.1.5.1 Viewing the Logs of IPs That Exceeded Concurrent Sessions Threshold

Step 1. Go to **Policy > Outgoing** and then set as shown below:

- Enter a value in the **Max. Concurrent Sessions per IP** field
- Click **OK**.

Comment:

Add Policy	
Source Address :	<input type="text" value="Inside Any"/>
Destination Address :	<input type="text" value="Outside Any"/>
Service :	<input type="text" value="Any"/>
Schedule :	<input type="text" value="----- None -----"/>
Authentication :	<input type="text" value="----- None -----"/>
VPN Trunk :	<input type="text" value="----- None -----"/>
<input checked="" type="checkbox"/> Permit all outgoing connections <input type="checkbox"/> Deny all outgoing connections	
Action :	Permit the selected: <input type="checkbox"/> Port 1 (LAN1) <input type="checkbox"/> Port 2 (LAN2) <input type="checkbox"/> Port 3 (Port3) <input type="checkbox"/> Port 4 (WAN2) <input type="checkbox"/> Port 5 (WAN1)
Reporting Mechanisms : Packet Logging : <input type="checkbox"/> Enabled Traffic Grapher : <input type="checkbox"/> Enabled	
Web Filter :	<input type="text" value="----- None -----"/>
Application Blocking :	<input type="text" value="----- None -----"/>

Advanced Settings

QoS :

----- None ----- ▼

Max. Bandwidth Per Source IP :

Downstream Kbps / Upstream Kbps (0: unlimited)

P2P Bandwidth Limits :

Downstream Kbps / Upstream Kbps (0: unlimited)

Max. Concurrent Sessions Per IP :

(1 - 99999, 0: unlimited)

Max. Concurrent Sessions :

(1 - 99999, 0: unlimited)

Traffic Quota per Session :

KB (1 - 999999, 0: unlimited)

Traffic Quota Per Source IP :

MB (1 - 999999, 0: unlimited)

Traffic Quota per Day :

MB (1 - 999999, 0: unlimited)

IP Redirection :

Port 1 (LAN1) :

Automatic ▼

Port 2 (LAN2) :

Automatic ▼

Port 3 (Port3) :

Automatic ▼

Port 4 (WAN2) :

Automatic ▼

Port 5 (WAN1) :

Automatic ▼

Help

OK Cancel

Creating a Policy to Limit the Maximum Concurrent Sessions

1 / 1

Go

Source	Destination	Service	Action	Options	Configuration	Priority
Inside Any	Outside Any	Any	✓		<div>Modify</div> <div>Remove</div> <div>Pause</div>	1 ▼

1 / 1

Go

New Entry

Policy Successfully Created

Step 2. Under **Monitoring > Logs > Concurrent Sessions**, it shows the logs of the concurrent sessions that have exceeded the specified value.

- To delete the logs, click the **Clear** button and then click **OK** in the confirmation window.

8.1.6 Quota

8.1.6.1 Viewing the Logs of IPs That Exceeded Traffic Quota

Step 1. Go to **Policy > Outgoing** and then set as shown below:

- Type a value in the **Quota per Source IP** field.
- Click **OK**.

Comment:

Modify Policy	
Source Address :	Inside Any ▼
Destination Address :	Outside Any ▼
Service :	Any ▼
Schedule :	----- None ----- ▼
Authentication :	----- None ----- ▼
VPN Trunk :	----- None ----- ▼
<input checked="" type="checkbox"/> Permit all outgoing connections <input type="checkbox"/> Deny all outgoing connections	
Action :	Permit the selected: <input type="checkbox"/> Port 1 (LAN1) <input type="checkbox"/> Port 2 (LAN2) <input type="checkbox"/> Port 3 (Port3) <input type="checkbox"/> Port 4 (WAN2) <input type="checkbox"/> Port 5 (WAN1)
Reporting Mechanisms : Packet Logging : <input type="checkbox"/> Enabled Traffic Grapher : <input type="checkbox"/> Enabled	
Web Filter :	----- None ----- ▼
Application Blocking :	----- None ----- ▼

8.1.7 Logging Settings

8.1.7.1 Archiving or Retrieving Logs Generated by MH-2300

Step 1. Go to **System > Configuration > Settings** and then set as shown below:

- Tick **Enable email notifications** and then configure the related settings.
- Tick **Enable syslog messages** and then configure the related settings.

Email Notification Settings		Help
<input checked="" type="checkbox"/> Enable email notifications		
Sender Address :	<input type="text" value="inesc@planet.com.tw"/>	(Max. 80 characters, ex. sender@mydomain.com)
SMTP Server :	<input type="text" value="mail.planet.com.tw"/>	(Max. 80 characters, ex. mydomain.com)
Email Address 1 :	<input type="text" value="inesc@planet.com.tw"/>	(Max. 80 characters, ex. user1@mydomain.com)
Email Address 2 :	<input type="text"/>	(Max. 80 characters, ex. user2@mydomain.com)
<input type="checkbox"/> Enable SMTP authentication		
Account Name :	<input type="text"/>	(Max. 60 characters)
Password :	<input type="password"/>	(Max. 60 characters)
Email Validity Test :	<input type="button" value="Send Test"/>	

Enabling Email Notifications

Syslog Message Settings	
<input checked="" type="checkbox"/> Enable syslog messages	
Syslog Host IP Address :	<input type="text" value="192.168.1.160"/> (ex. 192.168.1.1)
Syslog Port :	<input type="text" value="514"/> (1 - 65535, ex. 514)

Enabling Syslog Messages

Step 2. Go to **Monitoring > Logs > Settings** and then set as shown below:

Logging Settings

Email Alert Settings (Please configure Email Notification Settings under System > Configuration > Settings) [Help](#)

From SMTP Server : mail.planet.com.tw

To E-mail Address 1 : inesc@planet.com.tw

Syslog Message Settings (Please configure Syslog Message Settings under System > Configuration > Settings)

Please Enable syslog messages at [System] -> [Configuration] -> [Setting].

Traffic Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

Event Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

Connection Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

Application Blocking Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

Concurrent Sessions Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

Traffic Quota Log Settings

☒ Send logs by email

☒ Enable syslog messages

☒

Enable 
RSS
feeds

OK

Cancel

The Logging Settings

8.2 Traffic Grapher

This chapter will cover the operation of *Traffic Grapher*, which allows for viewing the statistical graphs of a WAN interface or a network policy.

- *WAN Traffic* provides the statistical graphs of traffic or packets that are processed through a network interface.
- *Policy-based Traffic* provides the statistical graphs of traffic or packets that are managed by a network policy.

Terms in Traffic Grapher

Statistical Graph


- Vertical axis indicates the network traffic or packets.
- Horizontal axis indicates the time.

Direction / Source / Destination / Service / Action

- The table headings of the network policies that the *Traffic Grapher* is enabled.

Time

- The statistical graphs are available in different time units, including minute, hour, day and week.

 Note	<p>The update intervals of statistical graphs are as follows:</p> <ul style="list-style-type: none"> ■ Minutes : Statistics are refreshed on a minutely basis. ■ Hours : Statistics are refreshed on a hourly basis. ■ Days : Statistics are refreshed on a daily basis. ■ Weeks : Statistics are refreshed on a weekly basis.
---------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Bits/sec/ Bytes/sec/ Utilization/ Accumulated (Total)

- The basic units of network traffic or packets are as follows:
 - ◆ **Bits/sec:** Data transmission is measured in bits per second.
 - ◆ **Bytes/sec:** Data transmission is measured in byte per second.
 - ◆ **Utilization:** Traffic or packets are shown by the proportion relative to the **Max. Downstream / Upstream Bandwidth** specified within a WAN interface.
 - ◆ **Accumulated (Total):** Traffic or packets are shown by the total traffic or packets accumulated.

8.2.1 WAN Traffic

Step 1. Under **Monitoring > Traffic Grapher > WAN Traffic**, the statistical graphs of a WAN interface are available in different time units.

- Click **Minutes** for statistics that are graphed per minute.
- Click **Hours** for statistics that are graphed per hour.
- Click **Days** for statistics that are graphed per day.
- Click **Weeks** for statistics that are graphed per week.

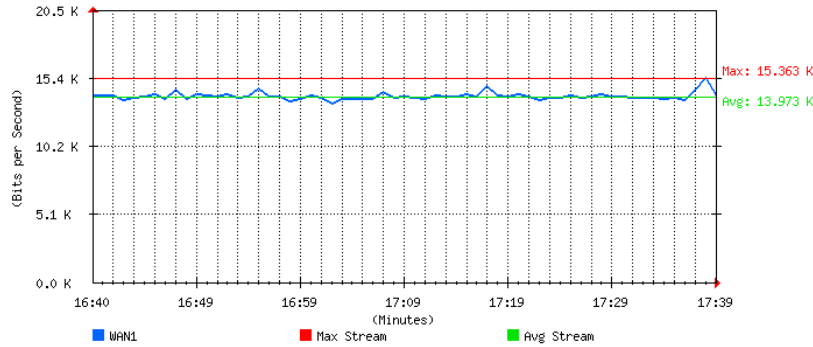
WAN	Time
WAN1	Minutes Hours Days Weeks Months Years
WAN2	Minutes Hours Days Weeks Months Years
WAN3	Minutes Hours Days Weeks Months Years
All WAN	Minutes Hours Days Weeks Months Years

The WAN Statistical Graphs Available on Different Time Bases

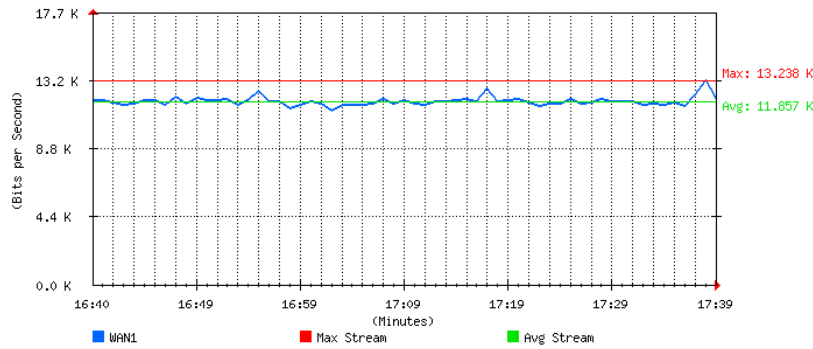
2010 / 12 / 21 17:00:00

Real-time: Down 6.51 KBits/sec Up 11.13 KBits/sec

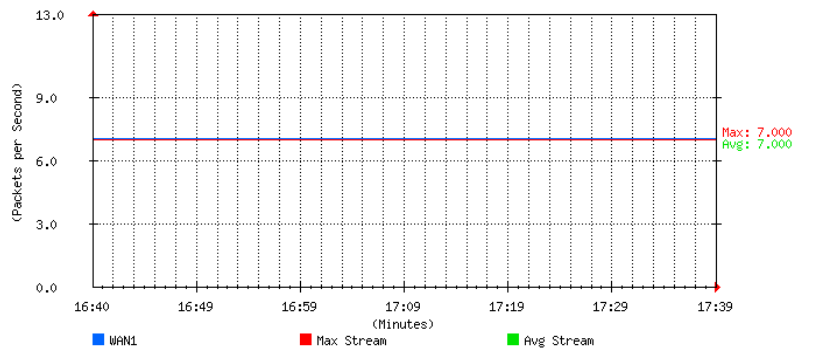
WAN1 Downstream



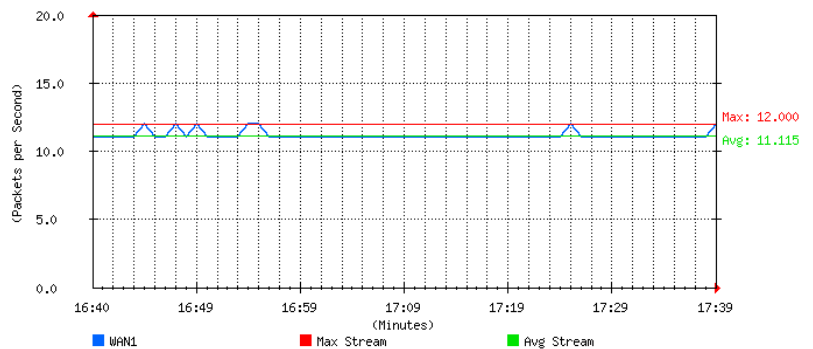
WAN1 Upstream




WAN1 Received Packets



WAN1 Transmitted Packets



The WAN Statistical Graphs



1. The **Traffic Grapher** is automatically activated after a WAN interface is added under **Network > Interface**.

2. The statistical graphs from a specific time can be obtained by using the date and time pickers (drop-down lists) and the **Refresh** button.

8.2.2 Policy-based Traffic

Step 1. Under **Monitoring > Traffic Grapher > Policy-Based Traffic**, the statistical graphs of a network policy are available in different time units (only if the **Traffic Grapher** is enabled within the policy):

- Click **Minutes** for the statistics that are graphed per minute.
- Click **Hours** for the statistics that are graphed per hour.
- Click **Days** for the statistics that are graphed per day.
- Click **Weeks** for the statistics that are graphed per week.
- Click **Months** for the statistics that are graphed per month.
- Click **Years** for the statistics that are graphed per year.

Type: All ▼ [Icons]

Type	Source	Destination	Service	Action	Time
Outgoing	Inside Any	Outside Any	Any	✓	Minutes Hours Days Weeks Months Years
Outgoing	Inside Any	Outside Any	Any	1	Minutes Hours Days Weeks Months Years

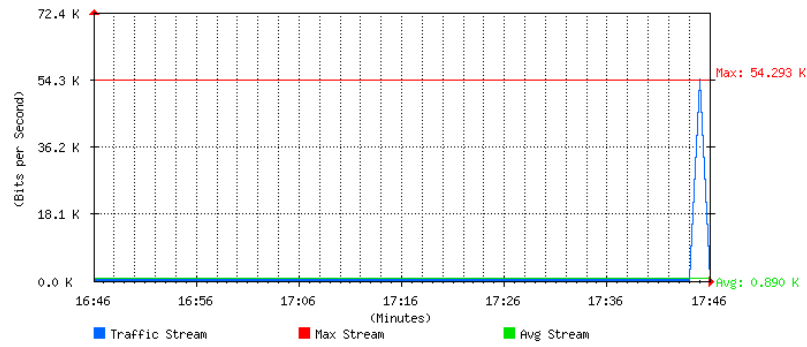
[Icons]

The Policy-based Statistical Graphs Available on Different Time Bases

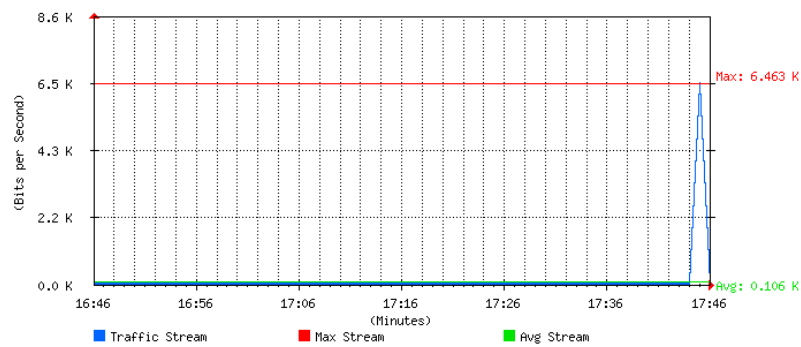
2010 / 12 / 21 17:-- --

Real-time: Down 0.0 Bits/sec Up 0.0 Bits/sec

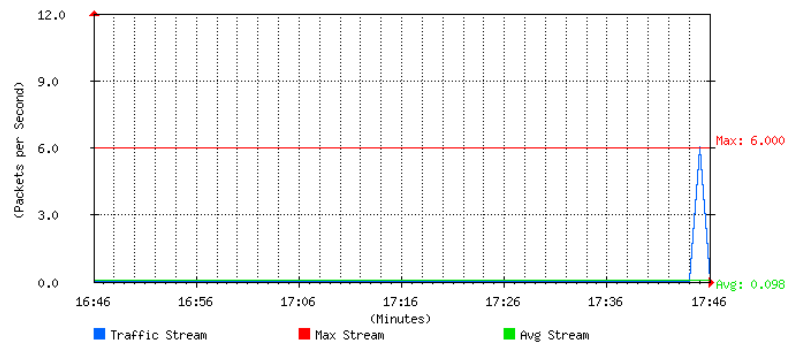
Downstream



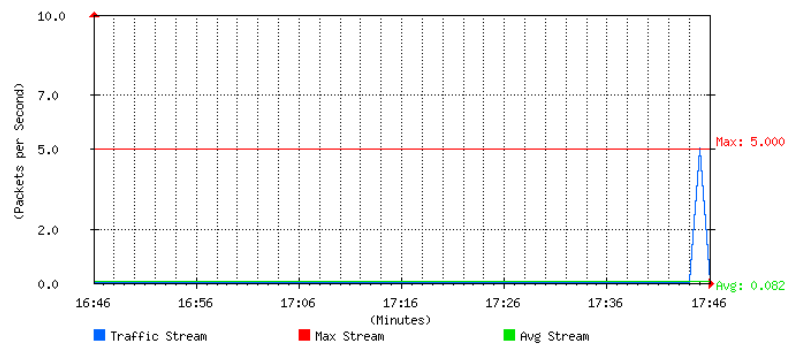
Upstream




Received Packets



Transmitted Packets



The Policy-based Statistical Graphs


Note

1. The **Traffic Grapher** requires manual activation for each network policy, respectively.
2. By traffic direction, statistical graphs are categorized into six types, namely outgoing, incoming, WAN-to-DMZ, LAN-to-DMZ, DMZ-to-WAN, DMZ-to-LAN, LAN-to-LAN, and DMZ-to-DMZ.
3. The statistical graphs from a specific time can be obtained by using the date and time pickers (drop-down lists) and the **Refresh** button.

8.3 Diagnostic Tools

The device provides Ping and Traceroute commands as well as a Web-based packet capture tool to help diagnose network issues with particular internal or external nodes.

8.3.1 Ping

Step 1. To test whether a host is reachable across an IP network, go to **Monitoring > Diagnostic Tools > Ping** and then configure as shown below:

- **Destination IP / Domain name** : Type the Destination IP or Domain name.
- **Packet Size** : Configure the size of each packet. (32 Bytes by default)
- **Count** : Configure the quantity of packets to send out. (4 by default)
- **Wait Time** : Specify the duration to wait between successive pings. (1 second by default)
- Select the interface from the **Interface** drop-down list.
- Click **OK**.

Ping Settings

Destination IP / Domain Name :	<input style="width: 90%;" type="text" value="8.8.4.4"/>	(Max. 30 characters)
Packet Size :	<input style="width: 40%;" type="text" value="32"/>	Byte(s) (1 - 9999)
Count :	<input style="width: 40%;" type="text" value="4"/>	(0 - 9999, 0: unlimited)
Wait Time :	<input style="width: 40%;" type="text" value="1"/>	second(s) (1 - 9999)
Interface :	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">WAN1</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">203.73.69.100</div> </div>	

Ping Result

Result
No data found!

The Parameters for Pinging a Host

Ping Settings

Destination IP / Domain Name : (Max. 30 characters)

Packet Size : Byte(s) (1 - 9999)

Count : (0 - 9999, 0: unlimited)

Wait Time : second(s) (1 - 9999)

Interface :

Ping Result

Result
PING 8.8.4.4 (8.8.4.4) from 203.73.69.100 : 32 bytes of data.
Reply from 8.8.4.4: bytes=32 icmp_seq=0 ttl=56 time=74 msec
Reply from 8.8.4.4: bytes=32 icmp_seq=1 ttl=56 time=44 msec
Reply from 8.8.4.4: bytes=32 icmp_seq=2 ttl=56 time=45 msec
Reply from 8.8.4.4: bytes=32 icmp_seq=3 ttl=56 time=44 msec
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 44.185/52.197/74.723/13.015 ms

The Ping Results of a Host



If VPN is selected from the **Interface** drop-down list, the user must enter the local LAN IP address in the **Interface** field. Enter the IP address that is under the same subnet range in the **Destination IP / Domain name** field.

- When the VPN connection is established between the local subnet (192.168.189.x/24) and remote subnet (192.168.169.x/24), the following method can be employed to test the packet transfer between the two subnets.

Ping Settings	
Destination IP / Domain Name :	<input type="text" value="192.168.80.100"/> (Max. 30 characters)
Packet Size :	<input type="text" value="32"/> Byte(s) (1 - 9999)
Count :	<input type="text" value="4"/> (0 - 9999, 0: unlimited)
Wait Time :	<input type="text" value="1"/> second(s) (1 - 9999)
Interface :	<input type="text" value="VPN-WAN3"/> <input type="text" value="192.168.1.1"/>
<input type="button" value="OK"/>	

Ping Result
Result
PING 192.168.80.100 (192.168.80.100) from 192.168.1.1 : 32 bytes of data.
Reply from 192.168.80.100: bytes=32 icmp_seq=0 ttl=128 time=161 msec
Reply from 192.168.80.100: bytes=32 icmp_seq=1 ttl=128 time=350 msec
Reply from 192.168.80.100: bytes=32 icmp_seq=2 ttl=128 time=171 msec
Reply from 192.168.80.100: bytes=32 icmp_seq=3 ttl=128 time=298 msec
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/mdev = 161.618/245.663/350.776/81.257 ms
<input type="button" value="Clear"/>

The Ping Results of a VPN Connection

8.3.2 Traceroute

Step 1. Under **Monitoring > Diagnostic Tools > Traceroute** the Traceroute command can be used by the MH-2300 to send out packets to a specific address to diagnose the quality of the traversed network.

- **Destination IP / Domain name** : Enter the destination address or domain name for the packets.
- **Packet Size** : Configure the size of each packet. (40 Bytes by default)
- **Max Time-to-Live** : Enter the maximum number of hops. (30 by default)
- **Wait Time** : Specify the duration to wait between successive pings. (2 seconds by default)
- **Interface** : Select the interface that the packets will originate from.
- Click **OK**.

Traceroute Settings	
Destination IP / Domain Name :	<input type="text" value="www.google.com"/> (Max. 30 characters)
Packet Size :	<input type="text" value="40"/> Bytes (40 - 9999)
Max Time-to-Live :	<input type="text" value="30"/> hops (1 - 255)
Wait Time :	<input type="text" value="2"/> seconds (2 - 9999)
Interface :	<input type="text" value="WAN1"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Traceroute Result		
<table border="1"> <thead> <tr> <th>Result</th> </tr> </thead> <tbody> <tr> <td>No data found!</td> </tr> </tbody> </table>	Result	No data found!
Result		
No data found!		

The Parameters for Tracerouting a Host

Traceroute Settings

Destination IP / Domain Name : (Max. 30 characters)
 Packet Size : Bytes (40 - 9999)
 Max Time-to-Live : hops (1 - 255)
 Wait Time : seconds (2 - 9999)
 Interface :

OK

Cancel

Traceroute Result

Result
traceroute: Warning: www.google.com has multiple addresses; using 64.233.183.103
traceroute to www.l.google.com (64.233.183.103), 30 hops max, 40 byte packets from 203.73.69.100
From 203.73.69.100
To hop 1 : IP = 203.73.69.1 round-trip min/avg/max = 42.029/43.243/44.981 ms
To hop 2 : IP = 192.72.179.253 round-trip min/avg/max = 38.604/43.282/51.054 ms
To hop 3 : IP = 139.175.57.133 round-trip min/avg/max = 39.590/40.318/41.611 ms
To hop 4 : IP = 139.175.59.202 round-trip min/avg/max = 39.353/57.380/90.323 ms
To hop 5 : IP = 74.125.51.81 IP = 74.125.51.77 round-trip min/avg/max = 39.985/47.805/59.437 ms
To hop 6 : IP = 209.85.243.26 round-trip min/avg/max = 40.616/44.233/48.470 ms
To hop 7 : IP = 209.85.250.103 IP = 209.85.243.21 round-trip min/avg/max = 40.910/41.772/42.501 ms
To hop 8 : IP = 72.14.238.42 IP = 72.14.238.222 IP = 72.14.238.42 round-trip min/avg/max = 45.190/52.136/57.317 ms
To hop 9 : IP = 64.233.183.103 round-trip min/avg/max = 42.749/45.027/48.377 ms
Traceroute complete

Clear

The Traceroute Results of a Host

8.4 Wake-on-LAN

Any wake-on-LAN supported PC can be remotely turned on by a "wake-up" packet sent from the MH-2300. By utilizing remote control software such as VNC, Terminal Service or PC Anywhere, a remote user may remotely wake up a computer and access it.

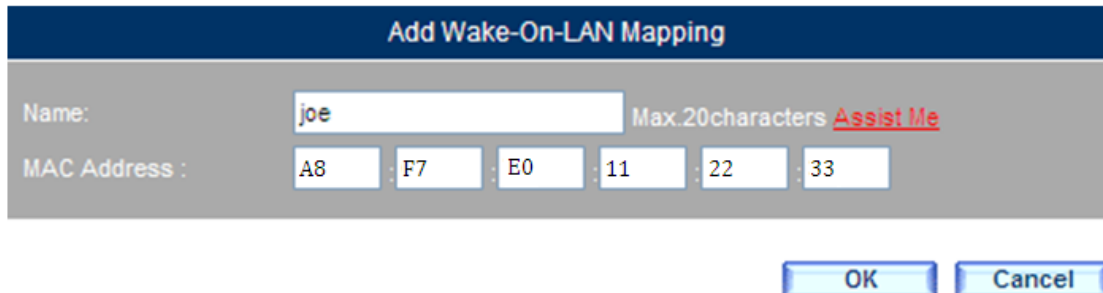
8.4.1 Example

8.4.1.1 Remote Controlling a LAN PC

Step 1. Supposing the MAC address of the PC that is desired to be remotely controlled is A8:F7:E0:B7:96:3B.

Step 2. Under **Monitoring > Wake-on-LAN > Settings**, click **New Entry** and then set as shown below:

- Enter the name in the field.
- Enter A8:F7:E0:B7:96:3B in the **MAC Address** field.
- Click **OK**.



The Wake-on-LAN Settings

Step 3. Click **WakeUp** to start up the PC.

Name ▲	MAC Address ▲	Configuration		
joe	A8:F7:E0:11:22:33	WakeUp	Modify	Remove

1 / 1 Go

New Entry

Clicking “WakeUp” to Start up the PC

8.5 Status


Status provides the current information about the device and the network including Interface, System Info, Authentication, ARP Table, Sessions Info, DHCP Clients, etc. as well as the current network connection status and various other information.

- **Interface:** Shows the status of each interface.
- **System Info:** Shows the utilization of CPU and memory.
- **Authentication:** Records the use of any authentication usage for the MH-2300.
- **ARP Table:** Records all the ARP tables of host PCs that have connected to MH-2300.
- **Sessions Info:** It records all the sessions sending or receiving packets over MH-2300.
- **DHCP Clients:** It records the status of IP addresses distributed by MH-2300 built-in DHCP server.

Terms in ARP Table

Search

- Available searching criteria are IP Version, Destination IP, MAC Address and Interface.

- ◆ Go to **Monitoring > Status > ARP Table**, click the search icon  and then set as below:
 - Select the **IP Version** and the **Interface**.
 - Click the **Search** button.

Search ARP Table

IP Version : IPv4 ▼

Destination IP : (ex. 192.168.1.1)

MAC Address :

Interface : WAN1 ▼

Search

Results

1 / 1 Go

Static <input type="checkbox"/>	Destination IP ▲	MAC Address ▲	Interface ▲	Configuration
<input type="checkbox"/>	192.168.1.160	00:e0:4c:77:11:98	WAN1	Remove
<input type="checkbox"/>	192.168.1.254	00:e0:4c:33:b9:3d	WAN1	Remove

1 / 1 Go

OK

Searching for an ARP Entry

Terms in Sessions Info

Search

- Available searching criteria are Direction, Priority, IP Version, Source IP, Destination IP and Port.
 - ◆ Under **Monitoring > Status > Sessions Info**, set as shown below:
 - Select "All" for **Direction**.
 - The **Priority** is set to "All" by default.
 - Select "IPv4" for **IP Version**.
 - Click **Search**.

Search Sessions Info Logs

Type : ▼
 Priority : ▼
 IP Version : ▼
 Source IP :
 Destination IP :
 Port : -> (1 - 65535)

[Search](#)


Results

<input type="checkbox"/>	IP Version	Connection Information	Start Time ▼	Traffic ▼	Type
No data found !					

Searching for the Info of a Session

Terms in DHCP Clients

Search

- Available searching criteria are IP Version, IP Addresses and MAC Address.
 - ◆ Under **Monitoring > Status > DHCP Clients**, click the search icon  and then set as shown below:
 - Select the **IP Version**.
 - Click **Search**.

Search DHCP Client

IP Version : ▼
 IP Addresses : (ex. 192.168.1.1)
 MAC Address :

[Search](#)

Results

IP Address ▲	MAC Address ▲	Leased Time	
		Start	End
No data found !			




























Searching for a DHCP-leased IP Address

8.5.1 Interface


Step 1. Under **Monitoring > Status > Interface**, it shows the status of all interfaces.

No. of Active Sessions : 270

System Uptime : 1 day(s) 3 hour(s) 17 min(s) 8 sec(s)

Physical Port No	1	2	3	4	5
Interface Designation	LAN1	LAN2	Port3	WAN2	WAN1
Connection Type	NAT	NAT	Disabled	Static IP	Static IP
Connection Status					
Link Speed	1000Mb/s				100Mb/s
Duplex Mode	Full				Full
Down-/Upstream BW (Mbps)				500 / 500	512 / 512
Downstream BW %					100%
Upstream BW %					100%
Connection Uptime					
MAC Address	00:11:22:33:44:3C	00:11:22:33:44:3D	00:11:22:33:44:3E	00:11:22:33:44:3F	00:11:22:33:44:40
IPv4 Address	192.168.0.1	192.168.3.1		210.66.155.79	192.168.1.162
Netmask	255.255.255.0	255.255.255.0		255.255.255.0	255.255.255.0
IPv4 Default Gateway				210.66.155.94	192.168.1.254
IPv6 Address					
Prefix Length					
IPv6 Default Gateway					
DNS Server 1				168.95.1.1	168.95.1.1
DNS Server 2				168.95.192.1	168.95.192.1
Rx Packets / Errors	36951,0	0,0	0,0	0,0	3624717,1
Tx Packets / Errors	30900,0	0,0	0,0	0,0	1650793,0
Ping/Tracert					
HTTP					
HTTPS					
Telnet					
SSH					

The Status of All Network Interfaces

 Note	1. System Uptime: The operating uptime of the MH-2300.
	2. No. of Active Sessions: Shows the current number of sessions connected to the device.
	3. Connection Type: Displays the interface connection mode.
	4. Connection Status: Shows the interface connection status.
	5. Up-/ Downstream BW (kbps): Shows the maximum downstream / upstream bandwidth set for the WAN interface (can be configured under Network > Interface > WAN).
	6. Downstream BW%: The percentage of downstream traffic to each WAN interface.
	7. Upstream BW%: The percentage of upstream traffic to each WAN interface.
	8. Connection Uptime: When the interface is connected using PPPoE, it displays the connection uptime.
	9. MAC Address: Displays the MAC address of the interface.

10. **IP Address / Netmask:** The interface's IP address and netmask.
11. **Default Gateway:** Shows the WAN gateway address.
12. **IPv6 Address / Prefix Length:** The interface's IPv6 address and prefix length.
13. **IPv6 Default Gateway:** The interface's IPv6 default gateway.
14. **DNS Server 1:** The DNS 1 server address from the ISP.
15. **DNS Server 2:** The DNS 2 server address from the ISP.
16. **Rx Packets / Errors:** Shows the quantity of received packets and the amount of error packets for each interface °
17. **Tx Packets / Errors:** Shows the quantity of sent packets and the amount of error packets for each interface.
18. **Ping / Tracert / HTTP / HTTPS/ Telnet/ SSH:** Shows whether the user can ping or tracert the device's interface, or access the Web UI through HTTP, HTTPS, Telnet or SSH.

8.5.2 System Info

Step 1. Under **Monitoring > Status > System Info**, it shows the current system information, such as CPU utilization and memory utilization.

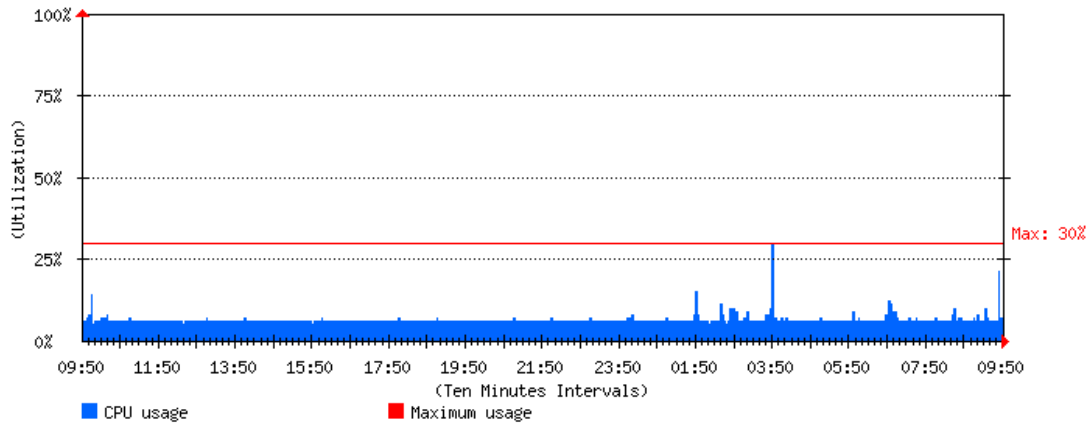
Memory Size : 128 MB

System Time : Tue, Dec 16 09:50:46 2014

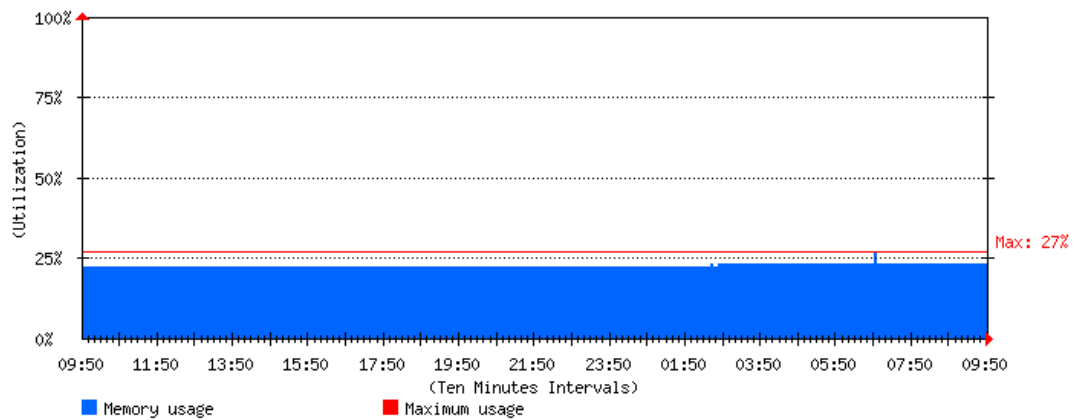
System Uptime : 1 day(s) 3 hour(s) 25 min(s) 31 sec(s)

Date : 2014-12-16 ▼

CPU Utilization



Memory Utilization




The Utilization of System Resources

8.5.3 Authentication

Step 1. Under **Monitoring > Status > Authentication**, it shows the authentication status of the device.

IP Address	Authentication-User Name ▲	Login Time ▲	Configuration
192.168.139.30	josh	2010/04/29 20:37:28	Remove

The Status of User Authentication

- 
 Note

1. **IP Address:** Displays the authenticated user's IP address.
 2. **Authentication – User Name:** The user's authenticated login name.
 3. **Login Time:** The user's login time (year/ month/ day/ hour/ minute/ second)

8.5.4 ARP Table

Step 1. Under **Monitoring > Status > ARP Table**, it shows **NetBIOS Name**, **Destination IP**, **MAC Address** and **Interface** of any computer that has connected to the device.

Anti-ARP Spoofing Software [Download](#) [Help](#)

IP Version : IPv4 




Static <input type="checkbox"/>	Destination IP ▲	MAC Address ▲	Interface ▲	Configuration
<input type="checkbox"/>	192.168.0.57	00:19:21:28:39:55	LAN1	Remove
<input type="checkbox"/>	192.168.1.160	00:e0:4c:77:11:98	WAN1	Remove
<input type="checkbox"/>	192.168.1.254	00:e0:4c:33:b9:3d	WAN1	Remove



[New Entry](#)
[OK](#)

The ARP Table

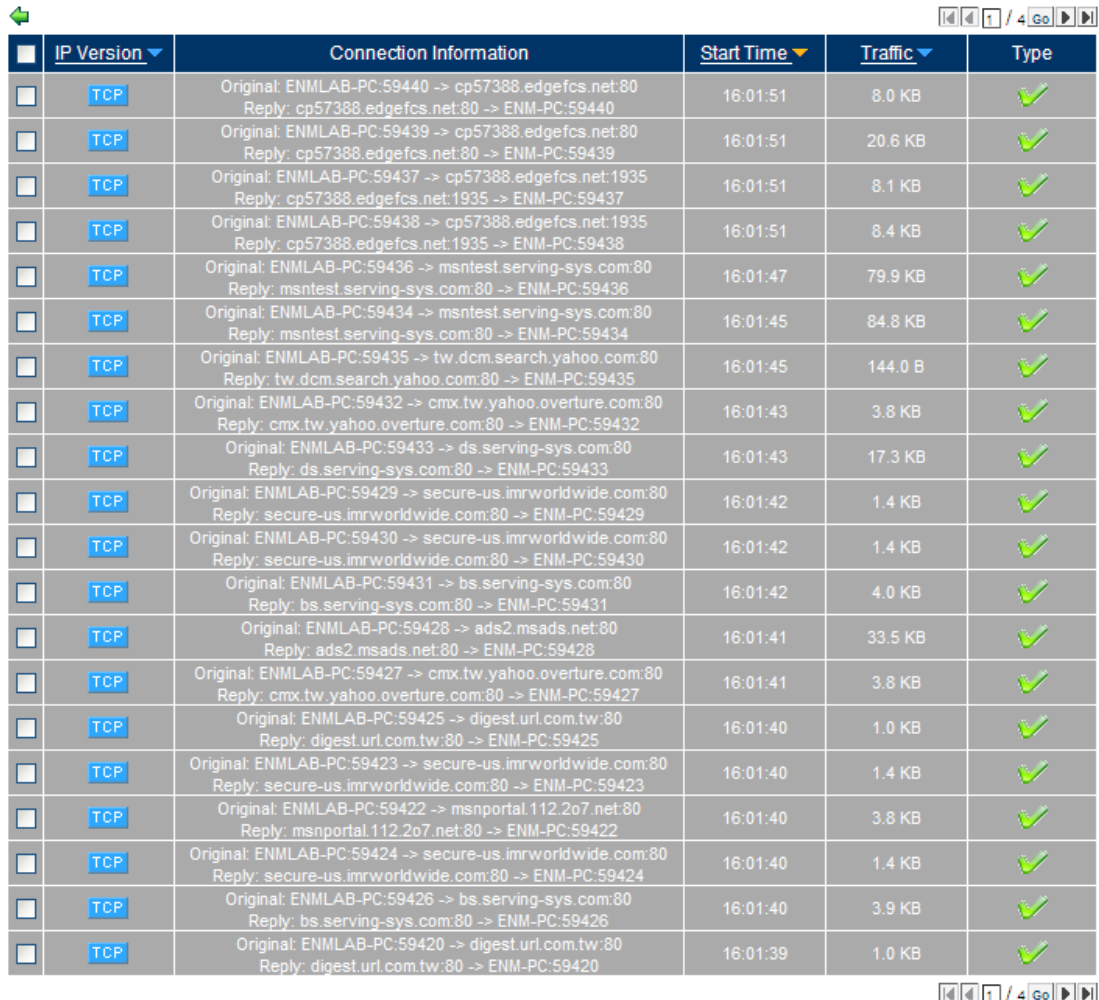
- 
 Note

1. **NetBIOS Name:** The computer's network identification name.
 2. **Destination IP:** The computer's IP address.
 3. **MAC Address:** The computer's network adapter identification number.
 4. **Interface:** The interface that the computer is connected to.
 5. To prevent any network packet errors, the **Static ARP Table** must coordinate with the **Anti-ARP virus software**. When these two function together, they provide a fixed mapping between the IP address and the MAC address.
 6. The **Anti-ARP Spoofing software** can be downloaded by clicking on the **Download** button. Once downloaded proceed with the following:
 - The program can be executed immediately to start taking effect against ARP viruses.
 - Copy the execution file to the computer's hard disk: \Documents and Settings\All Users\Start\Programs\Startup, after that, it will be executed every time when the system starts up.

8.5.5 Sessions Info

Step 1. Under **Monitoring > Status > Sessions Info**, it provides a list of all the sessions that have connected to the device.

- By clicking on any source IP, it shows the port number and the traffic.




IP Version	Connection Information	Start Time	Traffic	Type
TCP	Original: ENMLAB-PC:59440 -> cp57388.edgefcs.net:80 Reply: cp57388.edgefcs.net:80 -> ENM-PC:59440	16:01:51	8.0 KB	✓
TCP	Original: ENMLAB-PC:59439 -> cp57388.edgefcs.net:80 Reply: cp57388.edgefcs.net:80 -> ENM-PC:59439	16:01:51	20.6 KB	✓
TCP	Original: ENMLAB-PC:59437 -> cp57388.edgefcs.net:1935 Reply: cp57388.edgefcs.net:1935 -> ENM-PC:59437	16:01:51	8.1 KB	✓
TCP	Original: ENMLAB-PC:59438 -> cp57388.edgefcs.net:1935 Reply: cp57388.edgefcs.net:1935 -> ENM-PC:59438	16:01:51	8.4 KB	✓
TCP	Original: ENMLAB-PC:59436 -> msntest.serving-sys.com:80 Reply: msntest.serving-sys.com:80 -> ENM-PC:59436	16:01:47	79.9 KB	✓
TCP	Original: ENMLAB-PC:59434 -> msntest.serving-sys.com:80 Reply: msntest.serving-sys.com:80 -> ENM-PC:59434	16:01:45	84.8 KB	✓
TCP	Original: ENMLAB-PC:59435 -> tw.dcm.search.yahoo.com:80 Reply: tw.dcm.search.yahoo.com:80 -> ENM-PC:59435	16:01:45	144.0 B	✓
TCP	Original: ENMLAB-PC:59432 -> cmx.tw.yahoo.overture.com:80 Reply: cmx.tw.yahoo.overture.com:80 -> ENM-PC:59432	16:01:43	3.8 KB	✓
TCP	Original: ENMLAB-PC:59433 -> ds.serving-sys.com:80 Reply: ds.serving-sys.com:80 -> ENM-PC:59433	16:01:43	17.3 KB	✓
TCP	Original: ENMLAB-PC:59429 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59429	16:01:42	1.4 KB	✓
TCP	Original: ENMLAB-PC:59430 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59430	16:01:42	1.4 KB	✓
TCP	Original: ENMLAB-PC:59431 -> bs.serving-sys.com:80 Reply: bs.serving-sys.com:80 -> ENM-PC:59431	16:01:42	4.0 KB	✓
TCP	Original: ENMLAB-PC:59428 -> ads2.msads.net:80 Reply: ads2.msads.net:80 -> ENM-PC:59428	16:01:41	33.5 KB	✓
TCP	Original: ENMLAB-PC:59427 -> cmx.tw.yahoo.overture.com:80 Reply: cmx.tw.yahoo.overture.com:80 -> ENM-PC:59427	16:01:41	3.8 KB	✓
TCP	Original: ENMLAB-PC:59425 -> digest.url.com.tw:80 Reply: digest.url.com.tw:80 -> ENM-PC:59425	16:01:40	1.0 KB	✓
TCP	Original: ENMLAB-PC:59423 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59423	16:01:40	1.4 KB	✓
TCP	Original: ENMLAB-PC:59422 -> msnportal.112.2o7.net:80 Reply: msnportal.112.2o7.net:80 -> ENM-PC:59422	16:01:40	3.8 KB	✓
TCP	Original: ENMLAB-PC:59424 -> secure-us.imrworldwide.com:80 Reply: secure-us.imrworldwide.com:80 -> ENM-PC:59424	16:01:40	1.4 KB	✓
TCP	Original: ENMLAB-PC:59426 -> bs.serving-sys.com:80 Reply: bs.serving-sys.com:80 -> ENM-PC:59426	16:01:40	3.9 KB	✓
TCP	Original: ENMLAB-PC:59420 -> digest.url.com.tw:80 Reply: digest.url.com.tw:80 -> ENM-PC:59420	16:01:39	1.0 KB	✓

The Status of Active Sessions

8.5.6 DHCP Clients

Step 1. Under **Monitoring > Status > DHCP Clients**, it shows the status of IP address distributed by the device's DHCP server.

 <p>Note</p>	<ol style="list-style-type: none"> NetBIOS Name: The computer's network identification name. IP Address: The computer's IP address. MAC Address: The MAC address that the dynamic IP maps to. Leased Time: The start time and the end time of the dynamic IP. (year, month, day, hour, minute, second)
-------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------